インターネットを安全に使うための基本を学びませんか？

2025年9月24日（水）

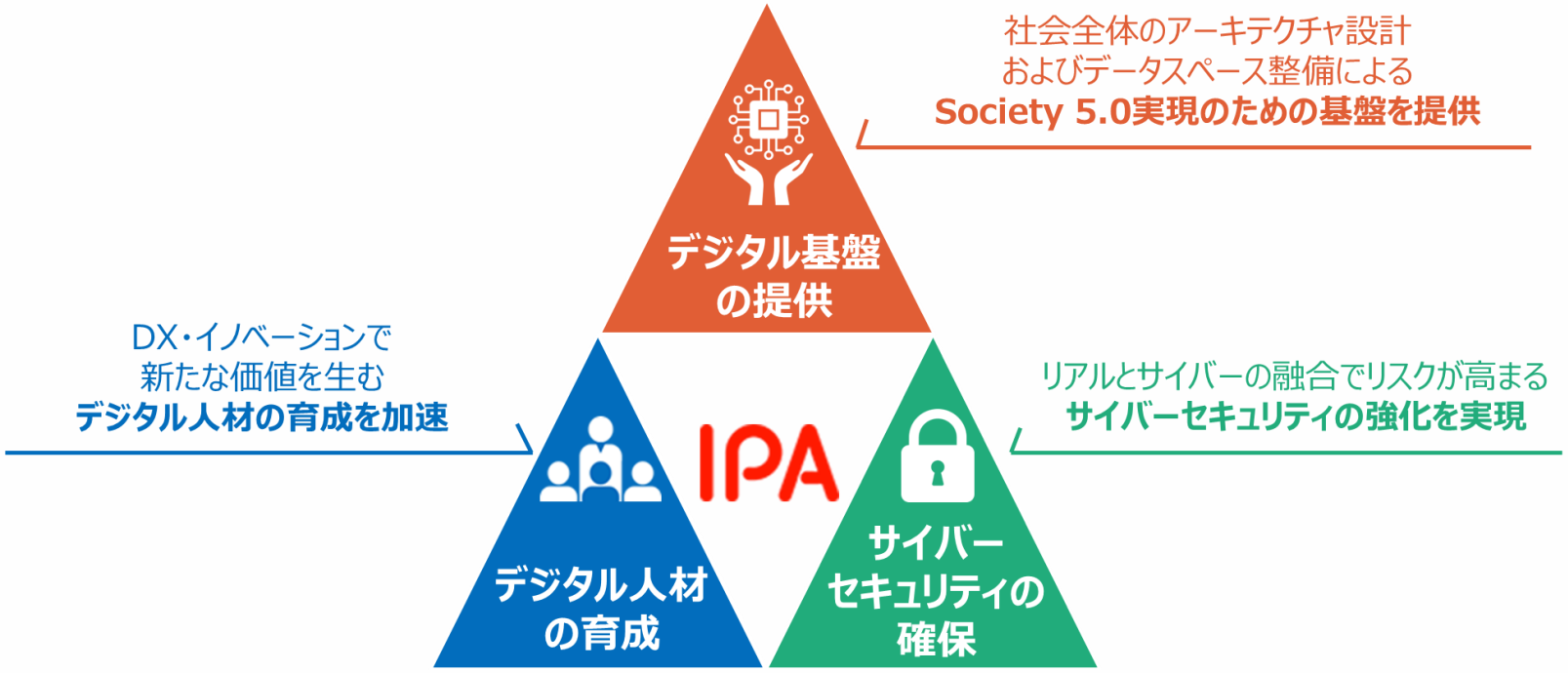
独立行政法人情報処理推進機構
セキュリティセンター 普及啓発・振興部
エキスパート 伊藤吉史

IPA Better Life with IT

独立行政法人 情報処理推進機構（IPA）について

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「 **頼れるIT社会** 」の実現を目指しています。

「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



■名称: 独立行政法人情報処理推進機構
(Information-technology Promotion Agency, Japan)
■設立: 2004年1月5日
（前身母体の設立は1970年10月1日）
■理事長: 齊藤 裕

セキュリティに関する業務概要

■ 平時からインシデント発生時まで、セキュリティマネジメントからオペレーションまでトータルな施策・対応を実施。

普及啓発・リテラシー対策

- 情報セキュリティ白書
- 地域・中小企業支援
- サプライチェーン支援
- セキュリティ安心相談窓口
  2024年　12,787件

サイバーセキュリティ CSお助け隊

累計宣言数
約40万組織

SECURITY ACTION
セキュリティ対策自己宣言

オペレーション（検知・分析・対処調整）

- ネットワーク監視（独法等）
- 情報共有枠組（攻撃情報・脆弱性）
- 国家支援型サイバー攻撃対策
- サイバー事故原因究明

JVN iPedia
脆弱性データベース
約520万アクセス/月

J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan

IPA J-CRAT
2011年創立　341件支援（2023年）

セキュリティ・マネジメント/技術評価認証

- 経営ガイドライン、中小企業ガイドライン
- ISOに基づく第三者認証/暗号
- クラウド安全性評価（ISMAP）
- 独法等監査、政府システム監査
- 重要インフラリスクアセスメント

31か国が
相互承認に参加

人材育成

- 中核人材育成プログラム
  累計435名受講（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  2004年度～累計1,073名が受講
- 国家資格「情報処理安全確保支援士」
  登録者数23,751名（2025年4月1日時点）
- セキュリティ・コンクール
  応募約５万点（2023年度）

自己紹介

■伊藤吉史（いとう　よしふみ）

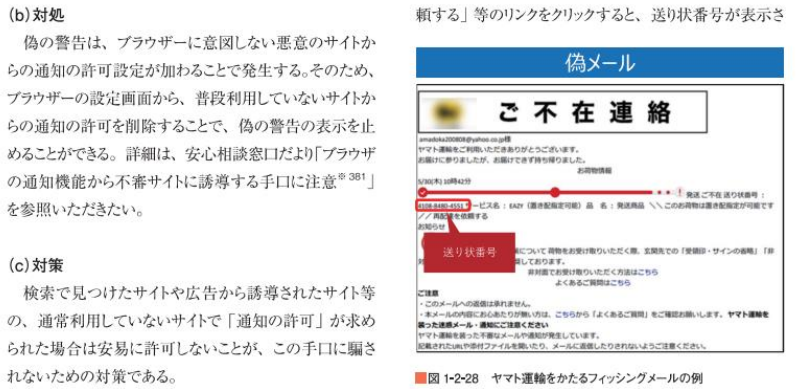
独立行政法人情報処理推進機(IPA)
セキュリティセンター 普及啓発・振興部　エキスパート
相談・支援グループ担当

・情報処理安全確保支援士（登録番号 020109)
・情報セキュリティ大学院大学 客員研究員

IPA**「情報セキュリティ安心相談窓口」**における情報セキュリティ関連相談への対応や、情報セキュリティ対策全般の普及啓発活動に従事。

ITベンダーで通信・金融関連システムのインテグレーション（SE)、品質保証業務を経て、情報セキュリティ大学院大学修了後　2020年4月より現職。

情報セキュリティ白書 2025 1.2.8章


(b) 対処
偽の警告は、ブラウザーに意図しない悪意のサイトからの通知の許可設定が加わることで発生する。そのため、ブラウザーの設定画面から、普段利用していないサイトからの通知の許可を削除することで、偽の警告の表示を止めることができる。詳細は、安心相談窓口だより「ブラウザの通知機能から不審サイトに誘導する手口に注意※381」を参照いただきたい。

(c) 対策
検索で見つけたサイトや広告から誘導されたサイト等の、通常利用していないサイトで「通知の許可」が求められた場合は安易に許可しないことが、この手口に騙されないための対策である。

頼する」等のリンクをクリックすると、送り状番号が表示さ

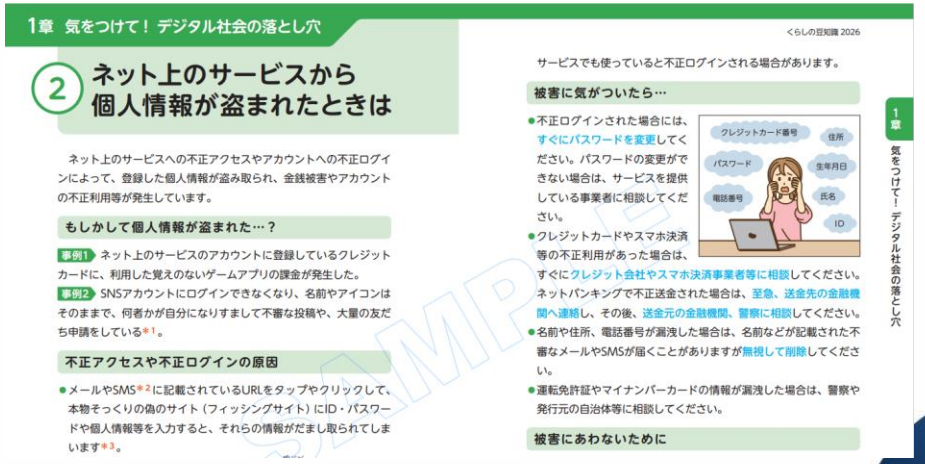
偽メール

ご 不 在 連 絡

送り状番号

■図 1-2-28　ヤマト運輸をかたるフィッシングメールの例

国民生活センター くらしの豆知識　2026年版


1章 気をつけて！ デジタル社会の落とし穴

くらしの豆知識 2026

② ネット上のサービスから個人情報が盗まれたときは

ネット上のサービスへの不正アクセスやアカウントへの不正ログインによって、登録した個人情報が盗み取られ、金銭被害やアカウントの不正利用等が発生しています。

もしかして個人情報が盗まれた…？

事例1 ネット上のサービスのアカウントに登録しているクレジットカードに、利用した覚えのないゲームアプリの課金が発生した。

事例2 SNSアカウントにログインできなくなり、名前やアイコンはそのままで、何者かが自分になりすまして不審な投稿や、大量の友だち申請をしている※1。

不正アクセスや不正ログインの原因

●メールやSMS※2に記載されているURLをタップやクリックして、本物そっくりの偽のサイト（フィッシングサイト）にID・パスワードや個人情報等を入力すると、それらの情報がだまし取られてしまいます※3。

サービスでも使っていると不正ログインされる場合があります。

被害に気がついたら…

●不正ログインされた場合には、すぐにパスワードを変更してください。パスワードの変更ができない場合は、サービスを提供している事業者に相談してください。

●クレジットカードやスマホ決済等の不正利用があった場合は、すぐにクレジット会社やスマホ決済事業者等に相談してください。ネットバンキングで不正送金された場合は、至急、送金先の金融機関へ連絡し、その後、送金元の金融機関、警察に相談してください。

●名前や住所、電話番号が漏洩した場合は、名前などが記載された不審なメールやSMSが届くことがありますが無視して削除してください。

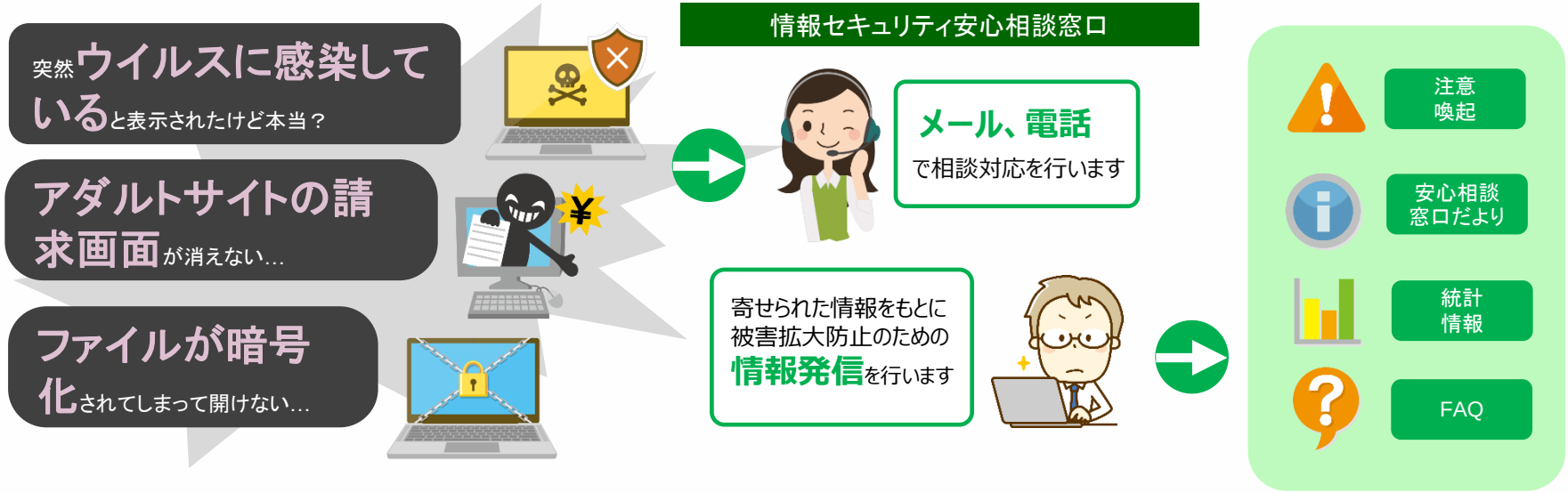
●運転免許証やマイナンバーカードの情報が漏洩した場合は、警察や発行元の自治体等に相談してください。

被害にあわないために

クレジットカード番号　住所　パスワード　生年月日　電話番号　氏名　ID

1章 気をつけて！ デジタル社会の落とし穴

IPA情報セキュリティ安心相談窓口



https://www.ipa.go.jp/security/anshin/about.html

電話
03-5978-7509
平日10:00-12:00 、13:30-17:00

メール
anshin@ipa.go.jp

ポータル
IPA安心相談 検索

目次

本日お伝えしたいこと

個人に対するインターネット上の最大の脅威は「ネット詐欺」

- 人の心理的な弱点に付け込み、被害者を騙すための道具として、既存のインターネットサービスやアプリを悪用
- サポート詐欺やフィッシングはその典型

ネット詐欺の対策

- 詐欺の**手口を知り「騙されない」**こと

ネット詐欺には代表的な手口がある

- 目次に示した**手口が主要なもの**

資料の構成

手口

手口についてその流れや仕組み、発生する被害について説明します。

対処

その手口にひっかかった場合に必要な対処を説明します。

対策

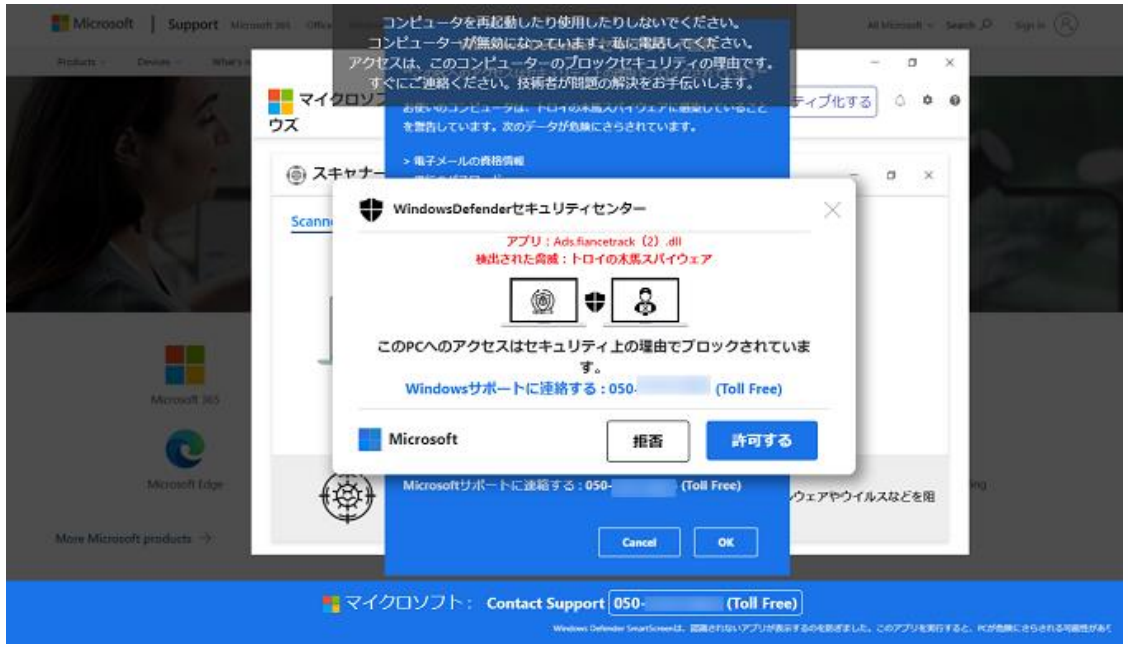
そもそも、その手口の被害にあわないための日ごろの対策について説明します。

1.サポート詐欺

1. サポート詐欺（偽のセキュリティ警告）

1.サポート詐欺

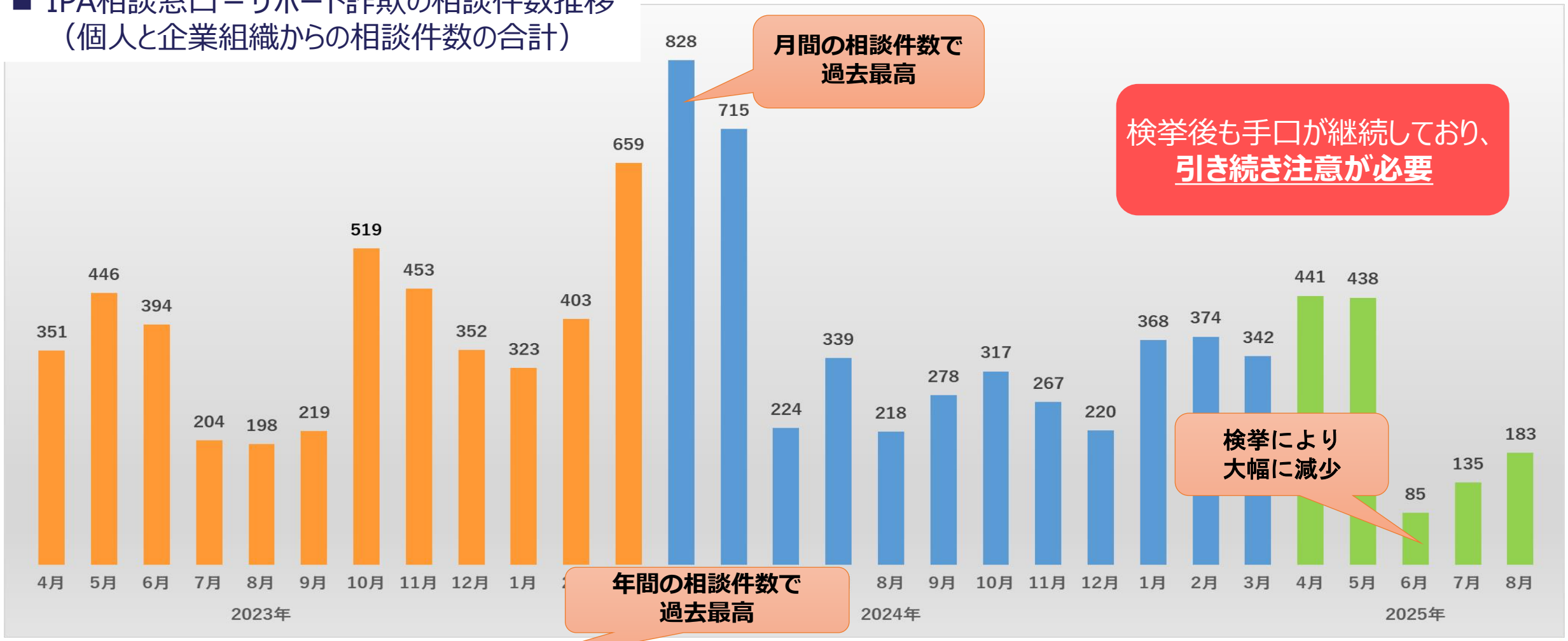
- パソコンでサイトを見ているときに、突然ウイルス感染の警告が表示される。



安心相談窓口だより
偽のセキュリティ警告に表示された番号に電話をかけないで！

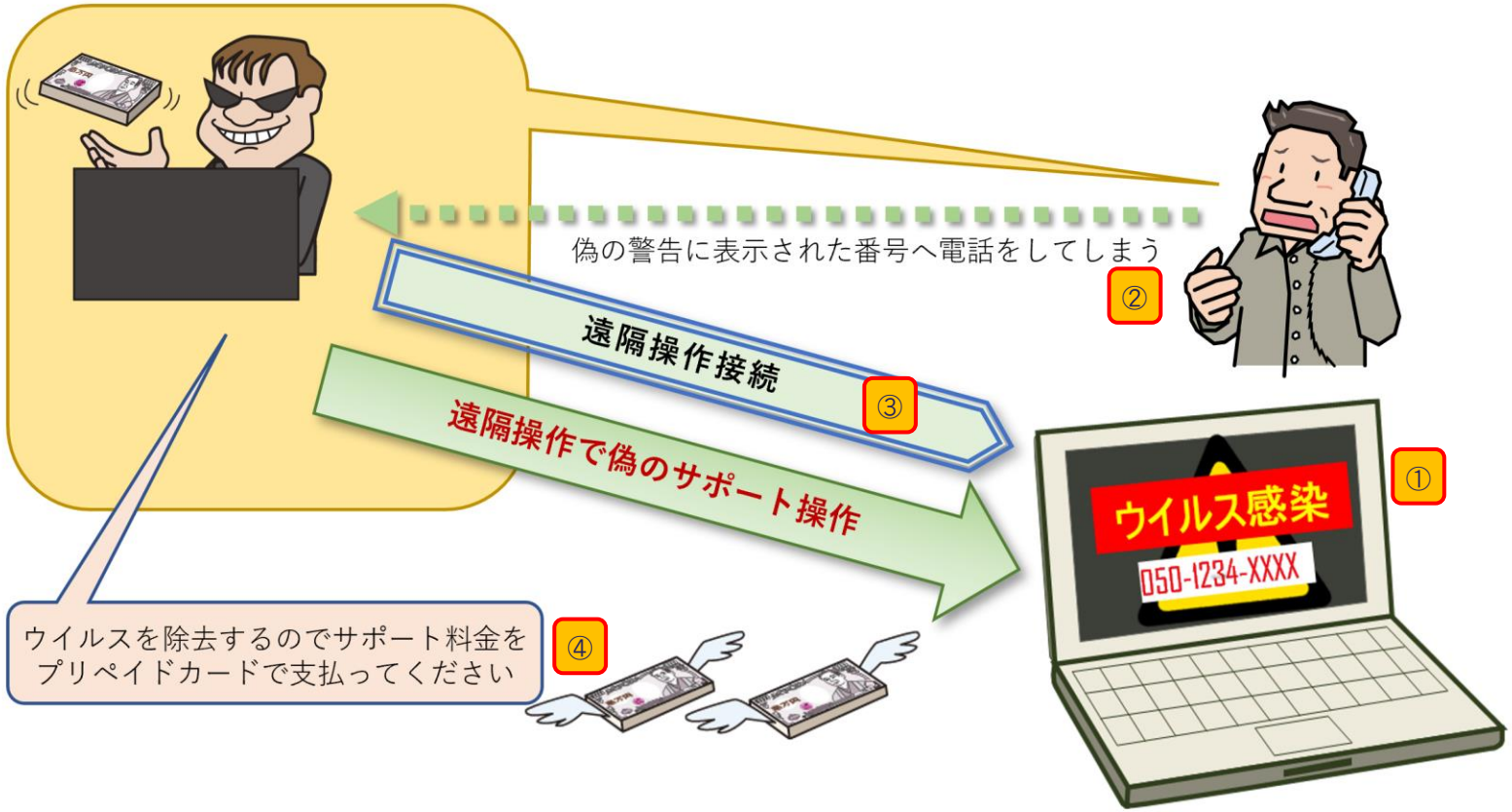
近年の月別相談件数（2023年4月～2025年8月）

■ IPA相談窓口－サポート詐欺の相談件数推移
（個人と企業組織からの相談件数の合計）



1.サポート詐欺

手口



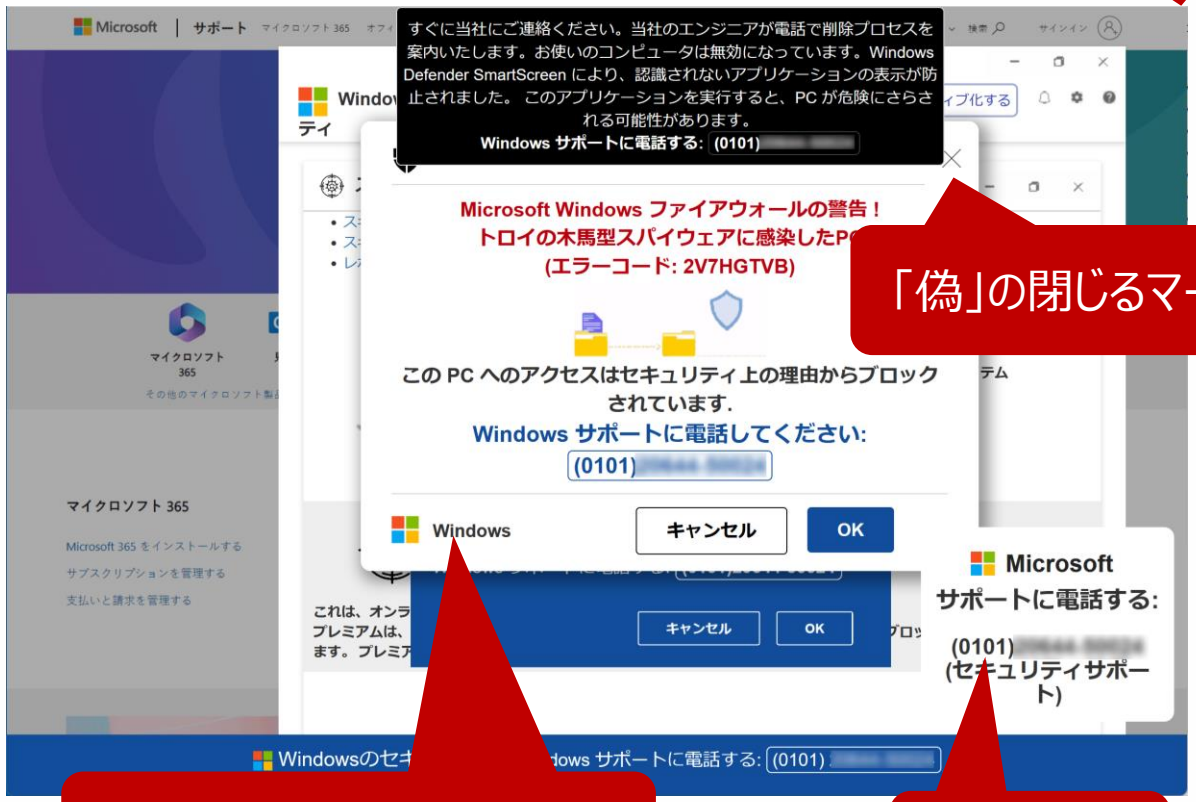
■ 手口の流れ

① パソコンに偽のウイルス感染警告が表示される。
② サポートに電話をする。
③ パソコンの遠隔操作へ誘導される。
④ うそのサポート料金を請求される。

1.サポート詐欺

手口

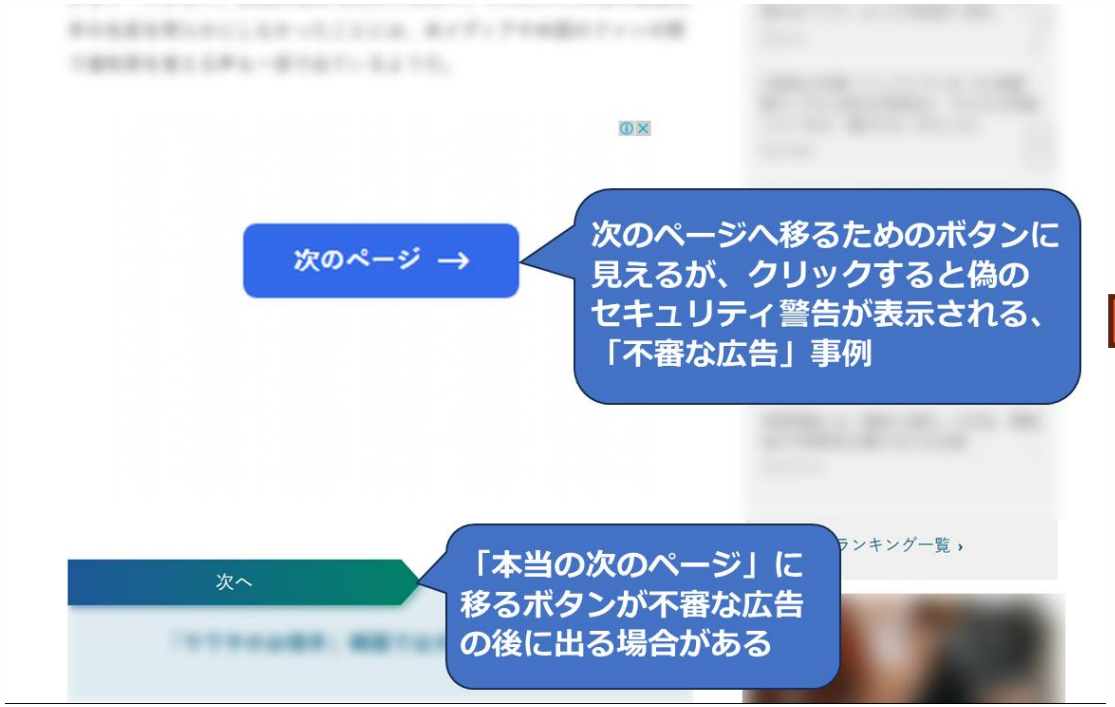
- 偽のセキュリティ警告画面

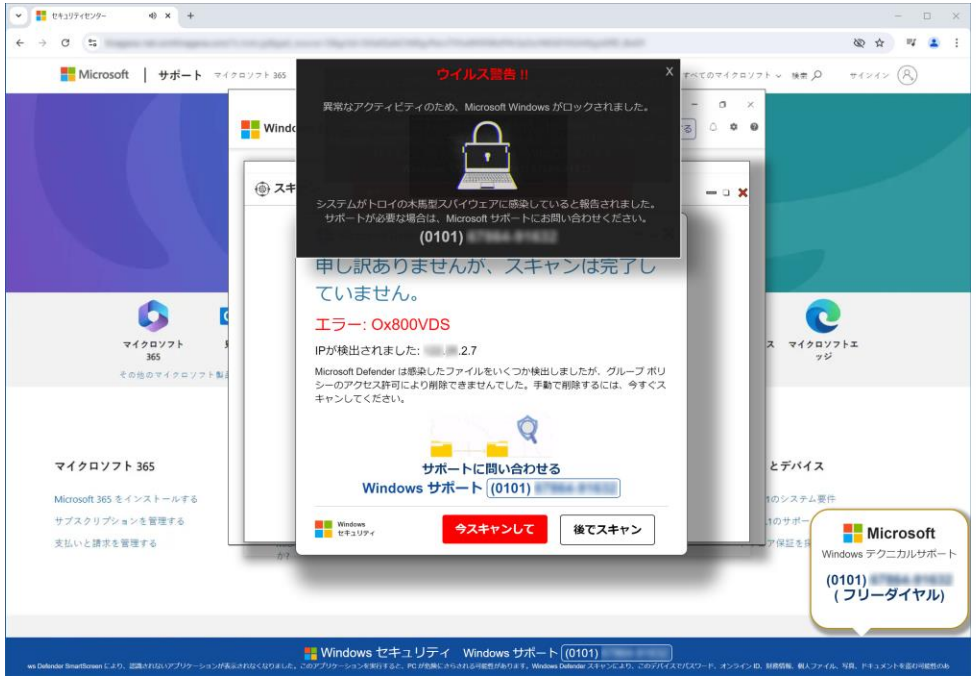


1.サポート詐欺 – 誘導されるきっかけ

- **普通のサイト**に表示されている**広告**からでる
- ネット検索の結果一覧からでる
- アダルトサイトなどからでる

このようなサイトを事前に把握することは困難。

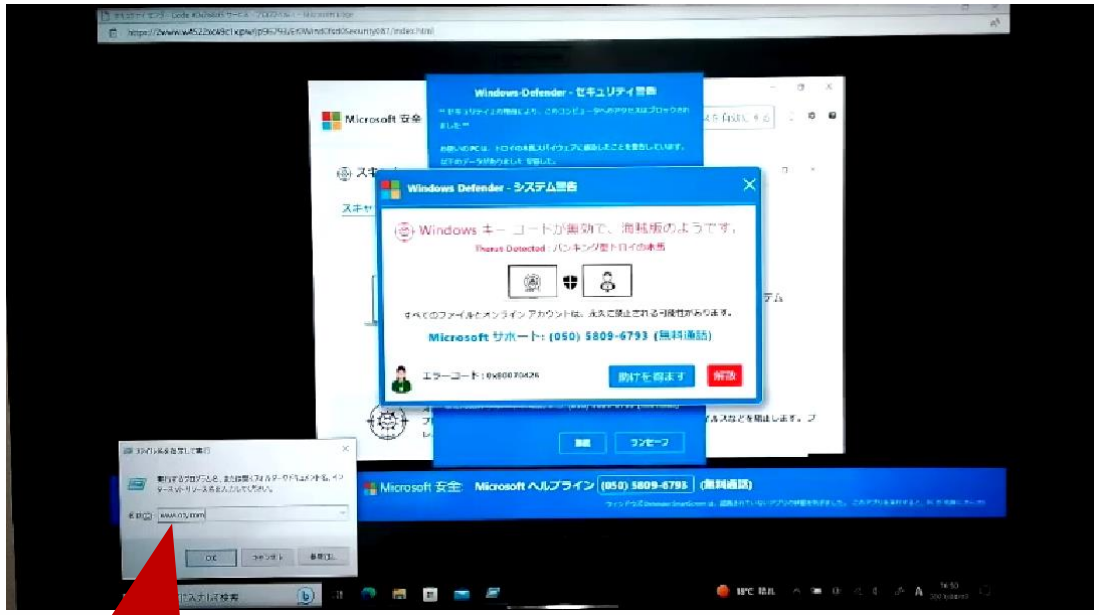




1.サポート詐欺

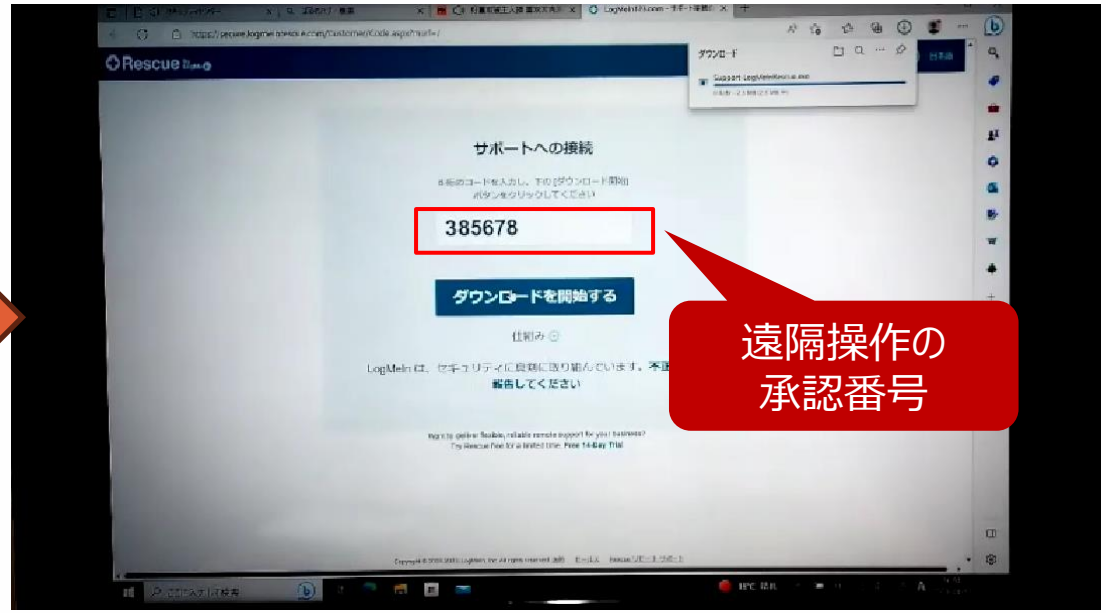
手口

■ 遠隔操作に誘導する画面（遠隔操作は始まっていない）



Win ＋ Rキーの操作を指示

遠隔操作ソフトのDL
サイトのURLを入力させる

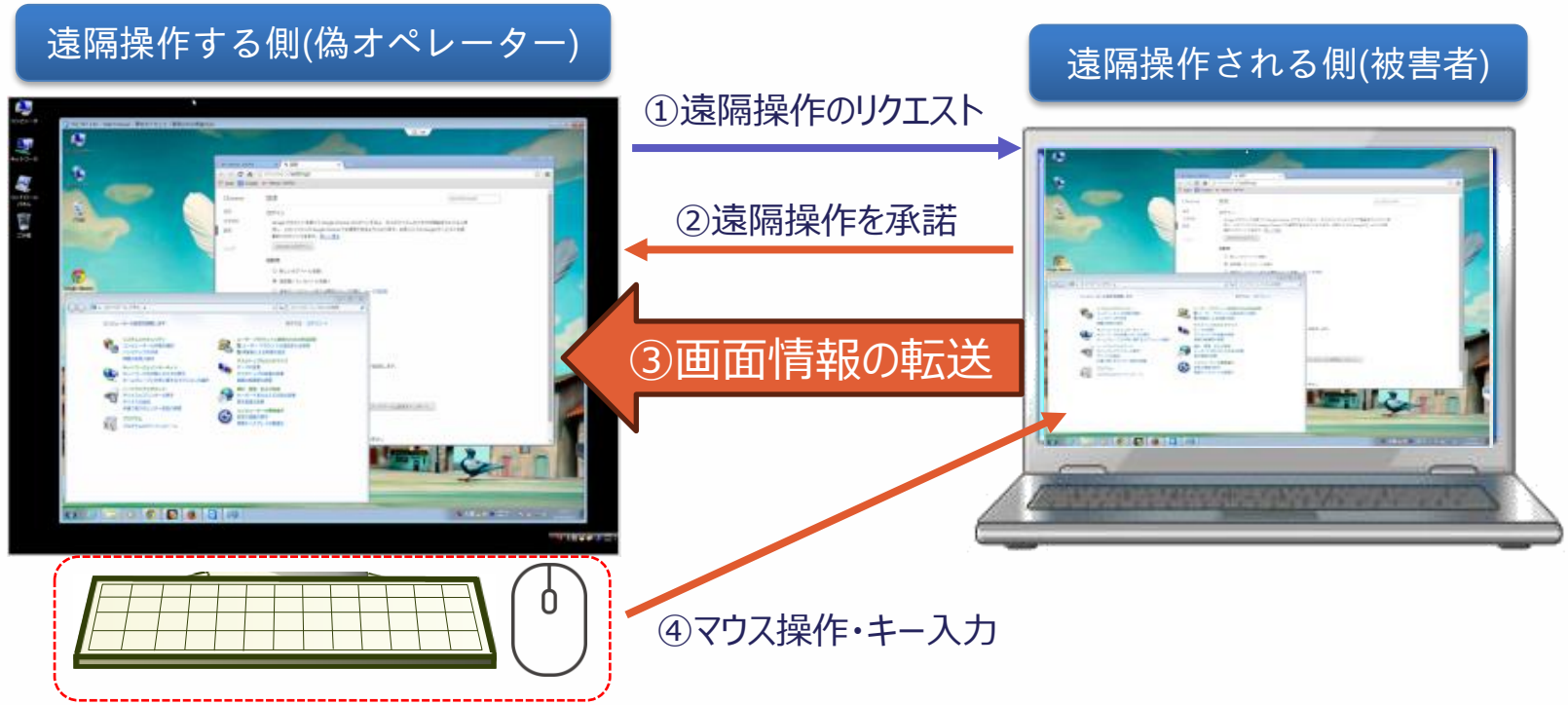


遠隔操作ソフトをダウンロードさせる画面

1.サポート詐欺

手口

■ 遠隔操作（サポート詐欺での悪用方法）



① 偽のオペレータから遠隔操作接続のリクエストが届く

② それを「承諾」するように指示され、**承諾する**

③ 遠隔操作接続が確立し、画面情報が相手に転送される

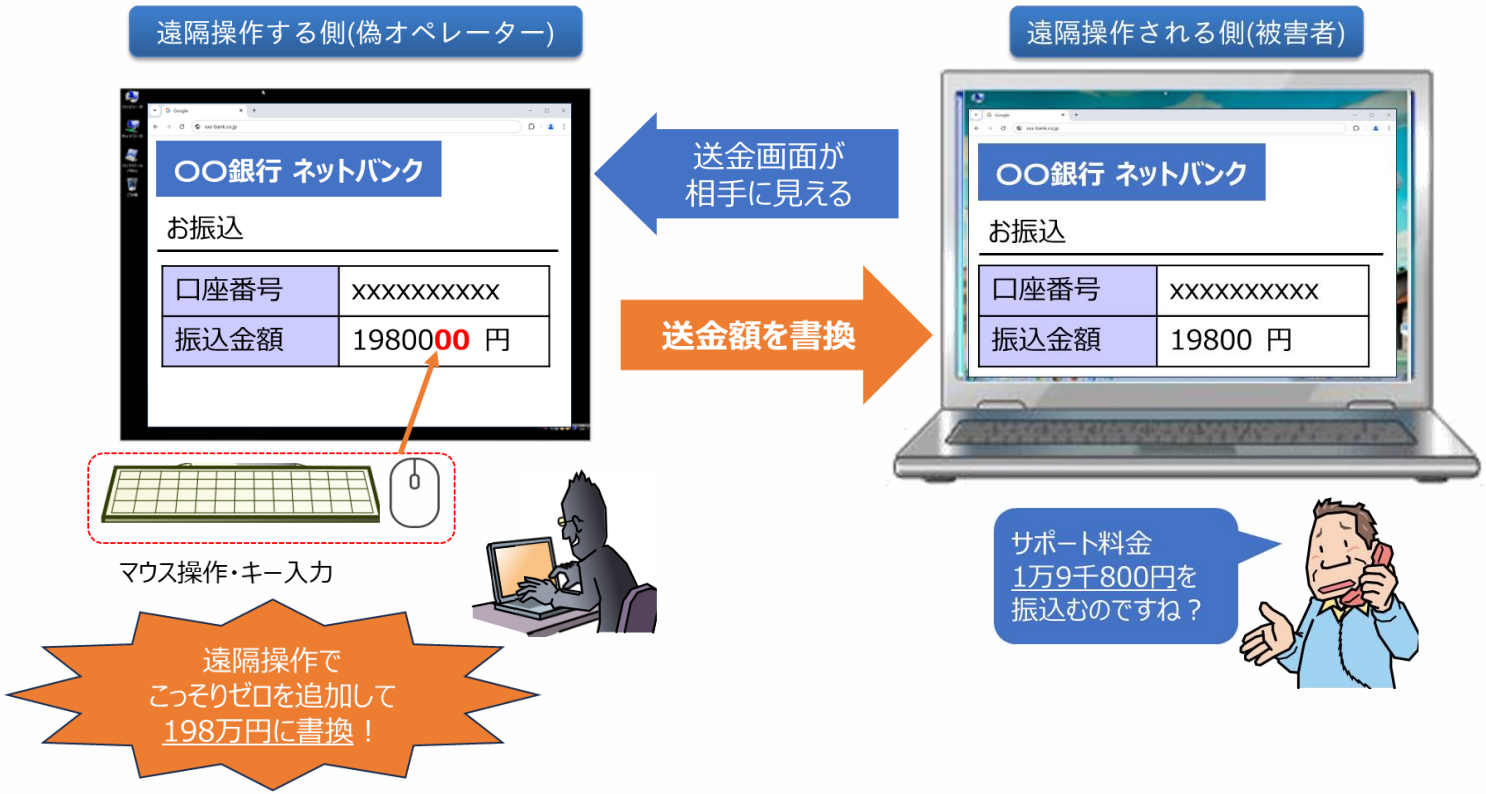
④ 相手から、被害者のパソコンのマウス操作・キー入力ができるようになる

遠隔操作中は、相手の操作内容が見える

1.サポート詐欺 – 遠隔操作を悪用した不正送金

手口

- 強引に有償サポート契約を勧める
- ネットバンキングを悪用して金銭を詐取する例

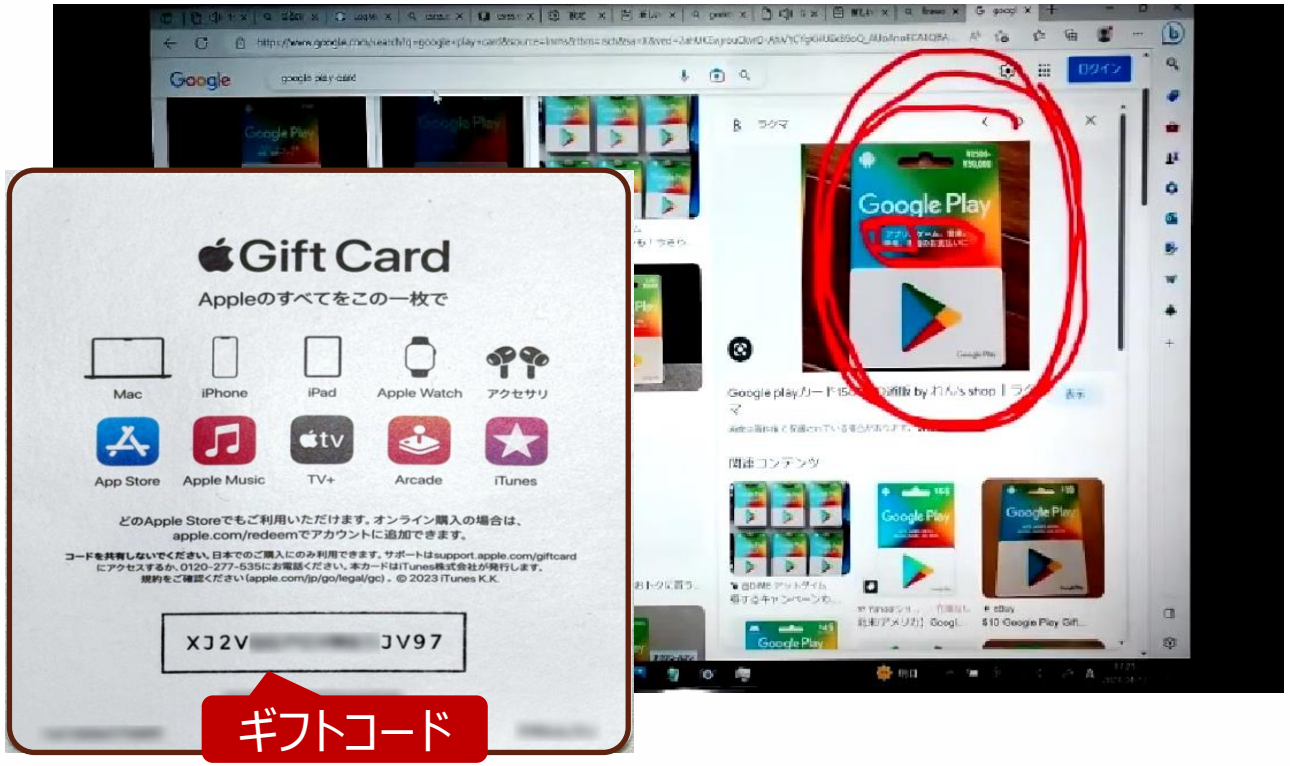


- **ネットバンキングにログイン**をさせて、遠隔操作を悪用した不正送金ケースが増えてきている（被害者の隙を見て送金額に0を追加するなど）。

1.サポート詐欺　プリペイドカードでの支払い

手口

- コンビニにプリペイドカードを買いに行くように指示する手口



- Google Playカード、Apple Store& iTunesカードを買わせることが多い
- カードを買ってくると「ギフトコード」聞き出して金銭を奪う
- 「コードが無効だ」などとでたらめを言って、繰り返し買いに行くことを指示する。

1.サポート詐欺 – 高額被害の事例

「あなたの口座を守るための作業を進めていきます。
口座情報を教えてください　→　**４２５０万円の被害**」

ABC ニュース　関西ニュース　KANSAI

11/21 20:57 配信

「パソコンがウイルスに感染」「口座を守るために口座情報教えて」　７６歳男性が約４２５０万円だまし取られる　大津市

大津市に住む７６歳の男性が、「あなたのパソコンがウイルスに感染しています」「口座情報やパスワードを教えてください」などのメッセージを信じて、現金約４２５０万円をだまし取られたとして、警察が多額詐欺事件として捜査しています。

警察によりますと１９日、大津市に住む会社役員の男性（７６）がパソコンを操作中、画面上に「トロイの木馬に感染しました。至急サポートセンターに電話をしてください」などとメッセージが表示されました。

男性が表示された連絡先に電話をかけたところ、応対した「大手ＩＴ会社の社員」を名乗る男２人から、「あなたのパソコンが悪質なコンピューターウイルスに感染しています」「このままではあなたの口座情報が流出し、口座からお金が盗まれます」「今から手続きをしていき

https://www.asahi.co.jp/webnews/pages/abc_28658.html

「３万５５００円　→　実際には
およそ**１１００万円をだまし取られていた**」

NHK　NHKについて　コロナ・感染症　ニュース

NEWS WEB　新着　天気　動画　特集　社会　気象・災害　科学・文化　政治　ビジネス　国際　スポー

三重 NEWS WEB

「サポート詐欺」で菰野町６０代女性が約１１００万円の被害

06月12日　18時55分

菰野町の６０代の女性が「Ｗｉｎｄｏｗｓがロックされました」などとうその話を持ちかけられ、指示に従ってパソコンを操作したところ、インターネットバンキングを悪用されて、合わせて１１００万円余りをだまし取られる被害があり、警察が特殊詐欺事件として捜査しています。

https://www3.nhk.or.jp/lnews/tsu/20240612/3070013049.html

1.サポート詐欺

対処

■ 偽のセキュリティ警告画面を閉じる

偽のセキュリティ警告画面の消しかた

簡単な操作方法

まずこの方法を試してください。

① ESC を2～3秒間押下します。（長押し）

② 偽の警告画面がひと回り小さい表示となり、ウィンドウの右上に『閉じるボタン』（×）が表示されますので、クリックしてください。

強制再起動による方法

左の操作で消せない場合に試してください。
遠隔操作中の場合はこの方法を推奨します。

① Ctrl と Alt と Delete を押下します。

② 画面右下の『電源ボタンアイコン』をクリックして、『再起動』を選択してください。
※再起動すると保存していないデータは失われる場合があります。

「ブラウザの閉じ方」の実施手順書

1.サポート詐欺

対処

- 偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト
- 画面の閉じ方が練習できます！！

体験サイトはパソコンでのみ実施できます

IPA　体験サイト　検索

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

1.サポート詐欺

対処

■ 遠隔操作ソフトのアンインストールとシステムの復元

- 当該ソフトウェアのアンインストールをしてください。アンインストールすることで遠隔操作ソフトは削除されます。
- **より安全な対処として「システムの復元」**を行い、不審なソフトをインストールする前の状態にパソコンを戻すことを推奨します。
- 「システムの復元」が実行できない場合はパソコンの初期化を推奨しています。
- 操作方法などはパソコンメーカーにお問い合わせください。

「アンインストール」の実施手順書

「システムの復元」の実施手順書

1.サポート詐欺

対策

■ 警告画面記載の電話番号に**電話をかけない**

- 正規のセキュリティサービスでは「警告表示に電話番号を表示して電話をかけさせてサポートを行う」ということは通常ありません。
- したがって、警告画面に表示された電話番号は正規なものでない可能性が高いため、決して電話をかけてはいけません。
- 一度でも電話をしてしまうと、電話番号が相手に伝わってしまい、後から電話がかかってきた事例があります。
- かかってきたとしても、着信拒否にするか出ないようにしてください。

■ 遠隔操作ソフトをダウンロードもインストールもしない

■ 購入・契約しない

2.フィッシング

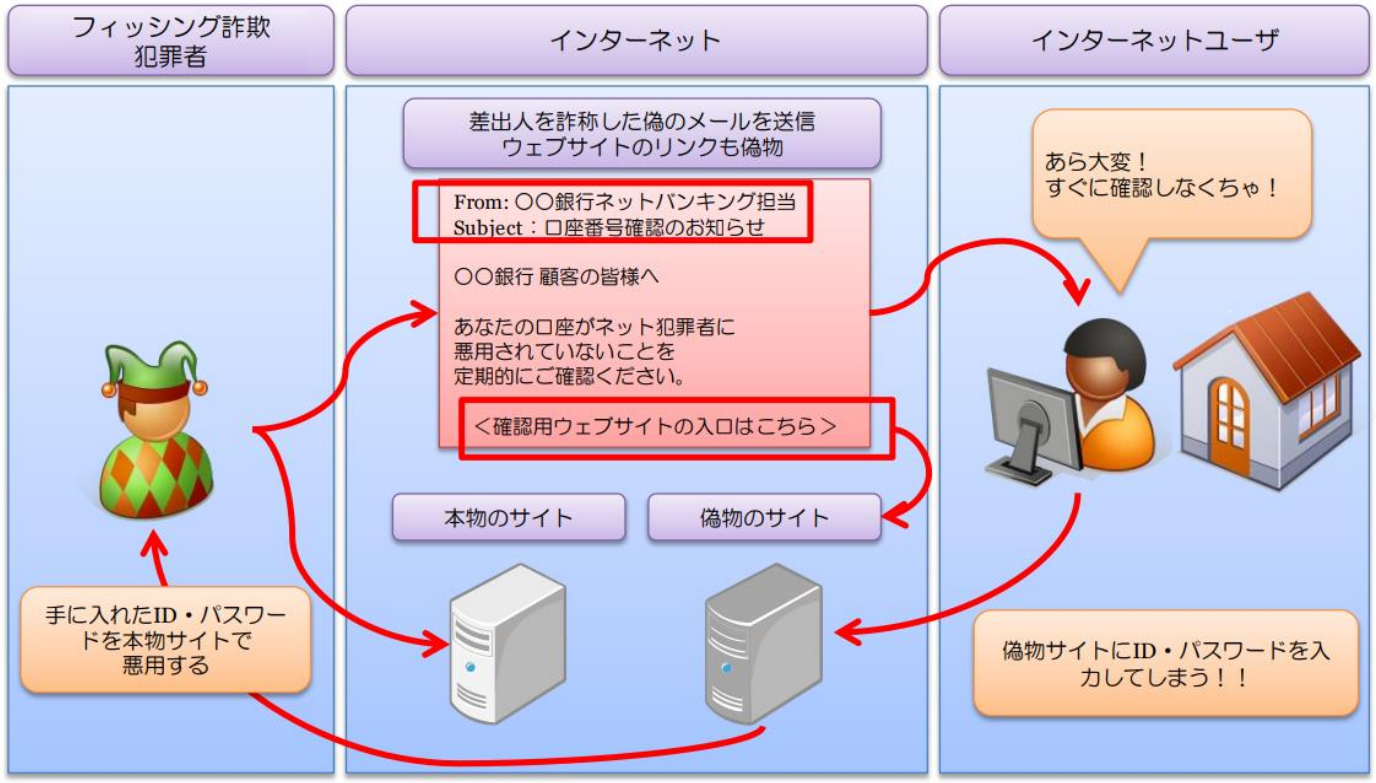
2.フィッシング

手口

■ フィッシング（Phishing）とは：

実在する組織をかたって、ユーザーネーム、パスワード、アカウント ID、ATM の暗証番号、クレジットカード番号といった個人情報を詐取すること。

- **本物そっくりの偽サイトをに誘導**して、個人情報を入力させて、それを奪います。
- フィッシングメールに以下の要素を入れて、受信した方にリンクをクリックさせようとします。
  - おどす（例：アカウントを凍結した）
  - よろこばせる、期待させる（例：当選した）



フィッシング対策協議会　利用者向けフィッシング対策ガイドライン
https://www.antiphishing.jp/report/guideline/

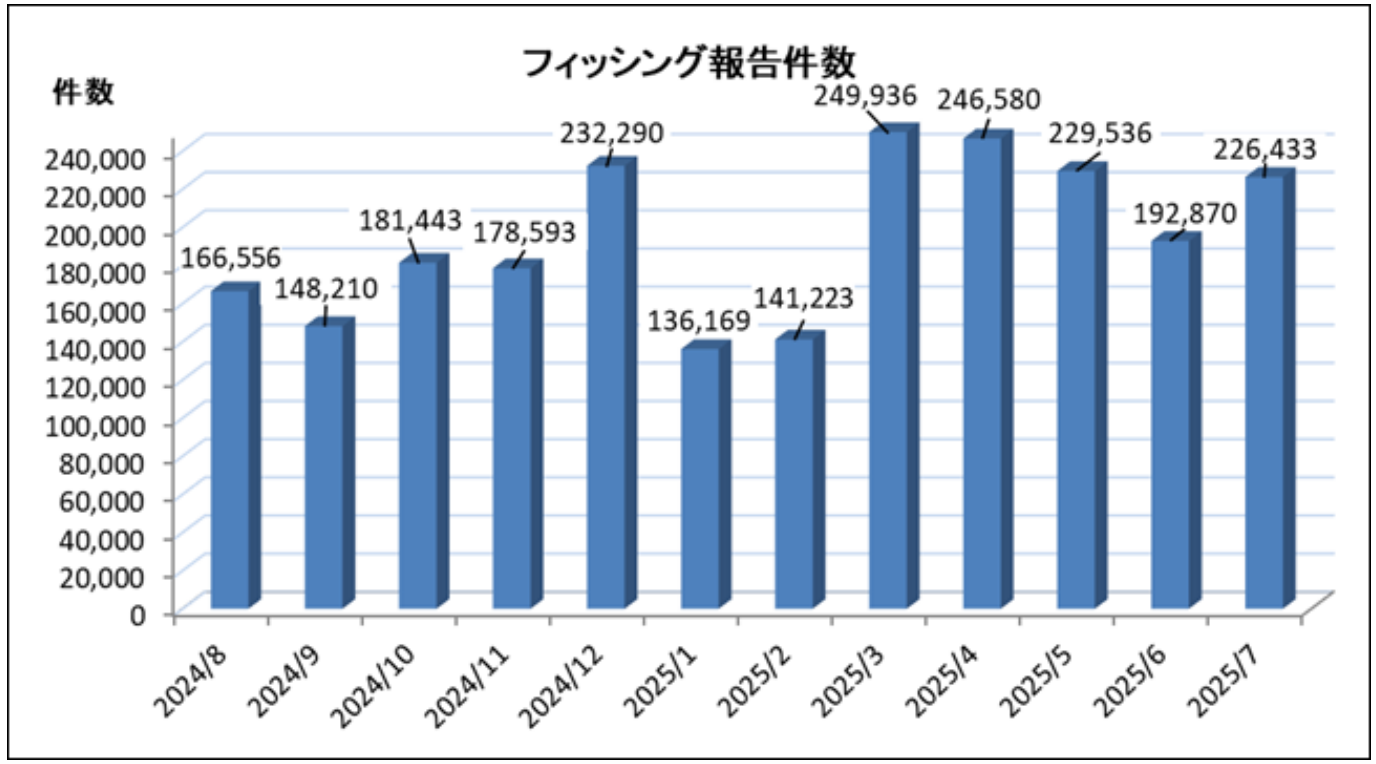
2.フィッシング　ある１日の不審メール

差出人	題名	受信日時
Marie Schmid	Late night, no limits 📍	2025/07/21 22:27
野村証券	【重要】本人確認情報の更新について（ご対応のお願い）	2025/07/21 22:27
PayPay銀行サポート佐藤	【PayPay銀行】不正利用防止についてのご案内	2025/07/21 21:33
国 税 庁	所得税納付について	2025/07/21 20:36
松井証券	「松井証券：異地ログインに関するご案内」	2025/07/21 20:11
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 18:47
myTOKYOGAS	【myTOKYOGAS】ご請求料金確定のお知らせ お客様のお支払い方法が承認されません	2025/07/21 18:39
DHL	重要なお知らせ：配達の試みが不成功である場合、出荷は送り主に返送されます。	2025/07/21 18:36
SBI証券	【安心サポート】お客様のアカウント確認について	2025/07/21 17:26
マネックスメール	【ご確認ください】ご利用環境に異常な接続を検知しました｜セキュリティ確認のお願い（マネックス証券）	2025/07/21 17:11
株式会社ビューカード	ご利用明細更新のお知らせ	2025/07/21 16:17
えきねっと	カード連携で「えきねっと」利用時のポイント2倍！お得な特典をゲット	2025/07/21 16:17
visajapan	【VISAカード】現在カードのご利用が一時停止されました	2025/07/21 15:34
株式会社ジャックス	<JACCS>2025年7月度お支払い金額確定のご案内	2025/07/21 15:28
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 14:22
ANAマイレージ サポートデスク	【ANA】マイル有効期限アラート	2025/07/21 12:56
えきねっと	会員情報更新と退会手続きのご案内	2025/07/21 12:51
ETC利用照会サービス事務局	ＥＴＣマイレージサービス仮登録完了	2025/07/21 12:43
American Express	[AMERICAN EXPRESS] ご請求金額確定のご案内	2025/07/21 12:30
<ANAショッピング A-style>	◤7/21(月)本日まで ◢ 会員様限定の最大20,000円OFFクーポンをお見逃しなく！	2025/07/21 12:11
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 12:02
佐川急便株式会社	ご不在連絡票に記載されている！Web再配達受付サービス！	2025/07/21 11:42
野村証券	【重要】本人確認情報の更新について（ご対応のお願い）	2025/07/21 10:58
国税電子申告.納税システム	【重要】税金未納に関する重要なお知らせ	2025/07/21 10:39
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 08:46
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 08:36
松井証券	「松井証券：取引制限に関するご案内」	2025/07/21 08:29
エポスカード	エポスカードからのお知らせ：お支払額のご案内	2025/07/21 07:13
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 06:23
ヤマト運輸【再配達のご案内】	【重要】配送情報確認のお願い	2025/07/21 06:19
ANAマイレージ サポートデスク	ANAマイレージ更新のご案内：失効予定マイルが発生しています	2025/07/21 06:05
東京ガスからのお知らせ	【myTOKYOGAS】ご請求料金確定	2025/07/21 05:48
ヨドバシ・ドット・コム	ヨドバシドットコム：「お客様情報」変更依頼受付のご連絡	2025/07/21 05:20
Emilia Baue	You'll like what's inside	2025/07/21 05:19
DHL EXPRESS	緊急 DHLの出荷が承認待ち	2025/07/21 05:17
ANAマイレージクラブ事務局	【重要】ANAマイレージクラブ：マイル加算手続きのご案内	2025/07/21 03:10
ANAマイレージクラブ事務局	【重要】ANAマイレージクラブ：マイル加算手続きのご案内	2025/07/21 02:20

2.フィッシング

- 2025 年 7月のフィッシング報告数は、226,433 件。
- 報告数全体のうち SBI証券 をかたるフィッシングは約 16.1 %、NTTドコモをかたるフィッシングは約 13.2 %といずれも増加。
- SMS から誘導されるフィッシング(スミッシング) については、7 月は全体的に報告が減少傾向ではあるものの、宅配便の不在通知を装う文面の報告が続いています。

フィッシング対策協議会に寄せられたフィッシング報告件数



https://www.antiphishing.jp/report/monthly/202507.html

2.フィッシング

手口

■ Amazonのフィッシング

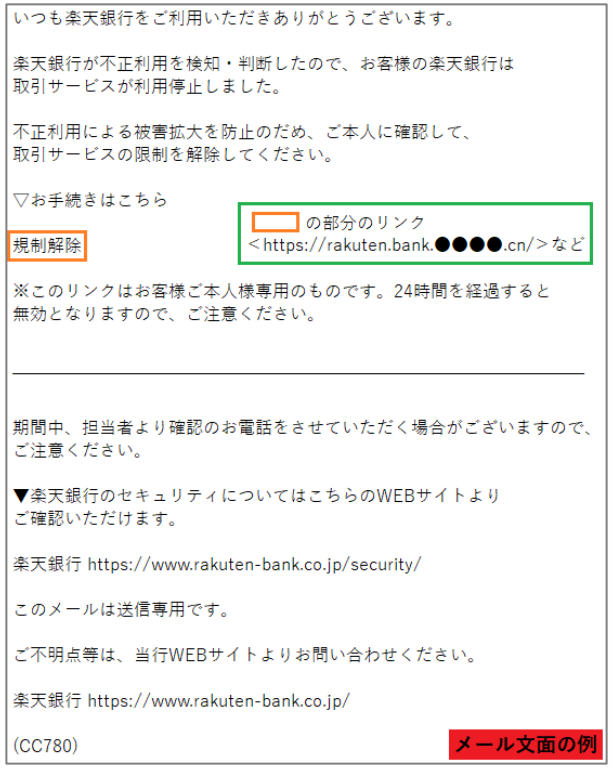
フィッシングメール

フィッシングサイト

URLリンクをクリックしない！！

パスワードの詐取

■ 楽天銀行のフィッシング



フィッシング対策協議会
https://www.antiphishing.jp/news/alert/

2.フィッシング – 証券会社を騙るフィッシングメール

手口

題名　：【設定必須】デバイス認証・FIDO認証のご案内（期限：5/31）
差出人　：SBI証券 認証<sbi_alert_master@pycwh.com>　アドレスブックに登録する
宛先　：[redacted]
添付ファイル　：text_html_1.html

証券会社が今まさに行っている認証強化の取り組みを逆手に取ったフィッシング

⇒ 手口が巧妙になっている

【重要】2025年5月31日より認証方式が義務化されます

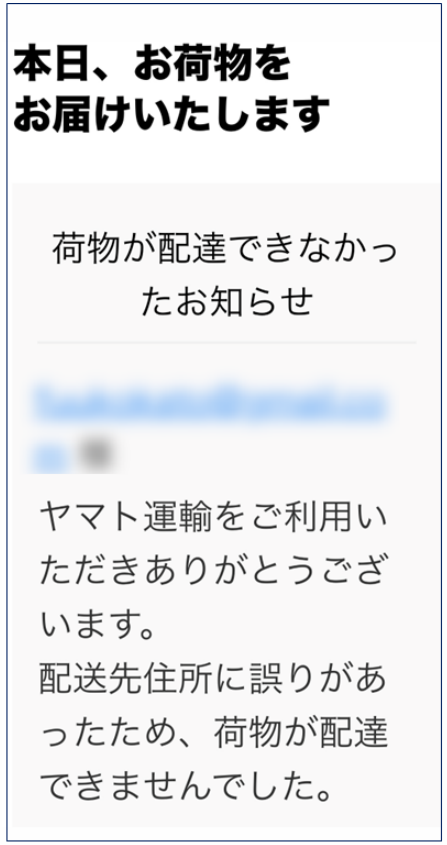
平素よりSBI証券をご利用いただき誠にありがとうございます。
当社ではお客様の資産と取引の安全性を確保するため、2025年5月31日（土）以降、ログイン時の多要素認証（デバイス認証・FIDO認証）を義務化いたします。
現在のご利用環境に関係なく、すべてのお客様に設定をお願いしております。
早期にご対応いただくことで、切替時の混乱を避け、スムーズにサービスをご利用いただけます。
※ 期限を過ぎた場合、ログイン・出金・注文など一部機能がご利用いただけなくなる可能性がございます。
特にスマートフォンからのご利用や、平日・営業時間中のお取引を予定されているお客様は、
余裕をもって事前にご対応くださいますようお願い申し上げます。

■ 設定期限
2025年5月31日（土） 23:59まで
■ 設定はこちら
メールアドレス登録および認証方式設定ページへ進む

IPAにて確認
2025.5.6

2.フィッシング – QRコードの悪用

手口



- 2024年8月以降、QRコードから偽サイトにアクセスさせるフィッシングメールの相談を受けています。
- スマートフォンでQRコードを長押しするとリンクにアクセスでき、フィッシングサイトに誘導される可能性があります。

IPAにて確認
2024.10.31

2.フィッシング – リアルタイムフィッシング

手口　リアルタイムフィッシング

- 偽のサイトに誘導　⇒　アカウント情報の入力 ⇒ 攻撃者がその場で正規サイトに入力
  二要素認証を突破する（ログイン画面にコードを入力させる場合は突破される）

攻撃者がすぐにID・パスワードを正規のサイトに入力する
⇒ **2要素認証コードが届く**

攻撃者がすぐに認証コードを正規のサイトに入力する
⇒ **不正ログイン**
二要素認証を突破

2.フィッシング – SMSによるフィッシング

- SMSによるフィッシング

不正なアプリのインストールに誘導する場合あり

安心相談窓口だより
宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中

【重要】三菱UFJ銀行お知らせ、お客様の銀行口座を一時凍結しています、ご本人様確認が必要となります。https://

「重要」みずほ銀行利用の緊急確認に関するお知らせ。ご確認が必要です。
https://t.co/

「重要」延滞金未払いによる電気供給停止予告とお支払手続き。https://

2.フィッシング – SMSによるフィッシング

- 偽SMS事例　銀行

- 銀行を騙り、ネットバンクの
  お客様番号とパスワードを奪う
- Android/iPhone共に偽サイト
  （フィッシングサイト）への誘導を確認
- 不正送金につながる可能性がある

2.フィッシング

対処

■ 受け取ったメールは削除

- メールを開いただけでは被害は発生しませんので、削除するだけで大丈夫です。
- メール本文のURLからフィッシングサイトにアクセスした場合でも、そのサイトで情報の入力等の操作をしていなければ基本的に被害は発生しません。
- 差出人アドレスや文面からの判断が困難で本物かどうか迷った場合には、メール内のURLや電話番号は使用せず、**公式サイトから真偽を確認**することをおすすめいたします。

■ フィッシングサイトで情報を入力してしまった場合

- ID・パスワードを入力した場合は、速やかにパスワードを変更してください。
- 入力したパスワードを他のサービスでも使いまわしている場合は、同様にパスワード変更を実施してください。
- クレジットカード情報を入力した場合は、速やかにクレジットカード会社に相談してください。
- オンラインバンキングのID・パスワードや関連情報を入力した場合は、速やかに銀行へ相談してください。
- その他、入力してしまった情報に関係するサービス提供企業に速やかに相談してください。

2.フィッシング

対策

■ 真偽がはっきりしないメールは無視して削除

- 記載のURLからウェブサイトにアクセスしない
- 添付ファイルを開かない
- 記載の電話番号に電話をしない
- 返信しない

■ 迷惑メールフィルターを使う

- フィッシングメールは迷惑メールの一種であり、迷惑メールフィルターでその多くが検知、分別、削除できます。
- ほとんどのメールサービスでは迷惑メールフィルターが利用できますが、標準では設定が無効となっていることが多いため、設定を確認し、有効にしましょう。
- メールアプリやセキュリティ対策ツールの迷惑メールフィルター機能も併用すると効果的です。
- しかし、迷惑メールを完全に止める方法はありませんので、自分自身の判断が最も大切です。

3. インターネットサービスへの不正ログイン

3.インターネットサービスへの不正ログイン

手口

- お笑いタレントやスポーツ選手のインスタグラムのアカウントを乗っ取ったとして32歳の容疑者が不正アクセス禁止法違反の疑いで逮捕された。警視庁は、乗っ取ったアカウントから女性に性的な画像を要求するメッセージなどを送っていた疑いがあるとみて調べている。
- 容疑者は、ほかにも別の俳優など男女4人のアカウントを乗っ取ったとして、すでに逮捕・起訴されていて、いずれも氏名や生年月日からパスワードを推測し、アカウントにアクセスしていたとみられている。

お笑いタレントらのインスタグラム乗っ取ったか 容疑者逮捕

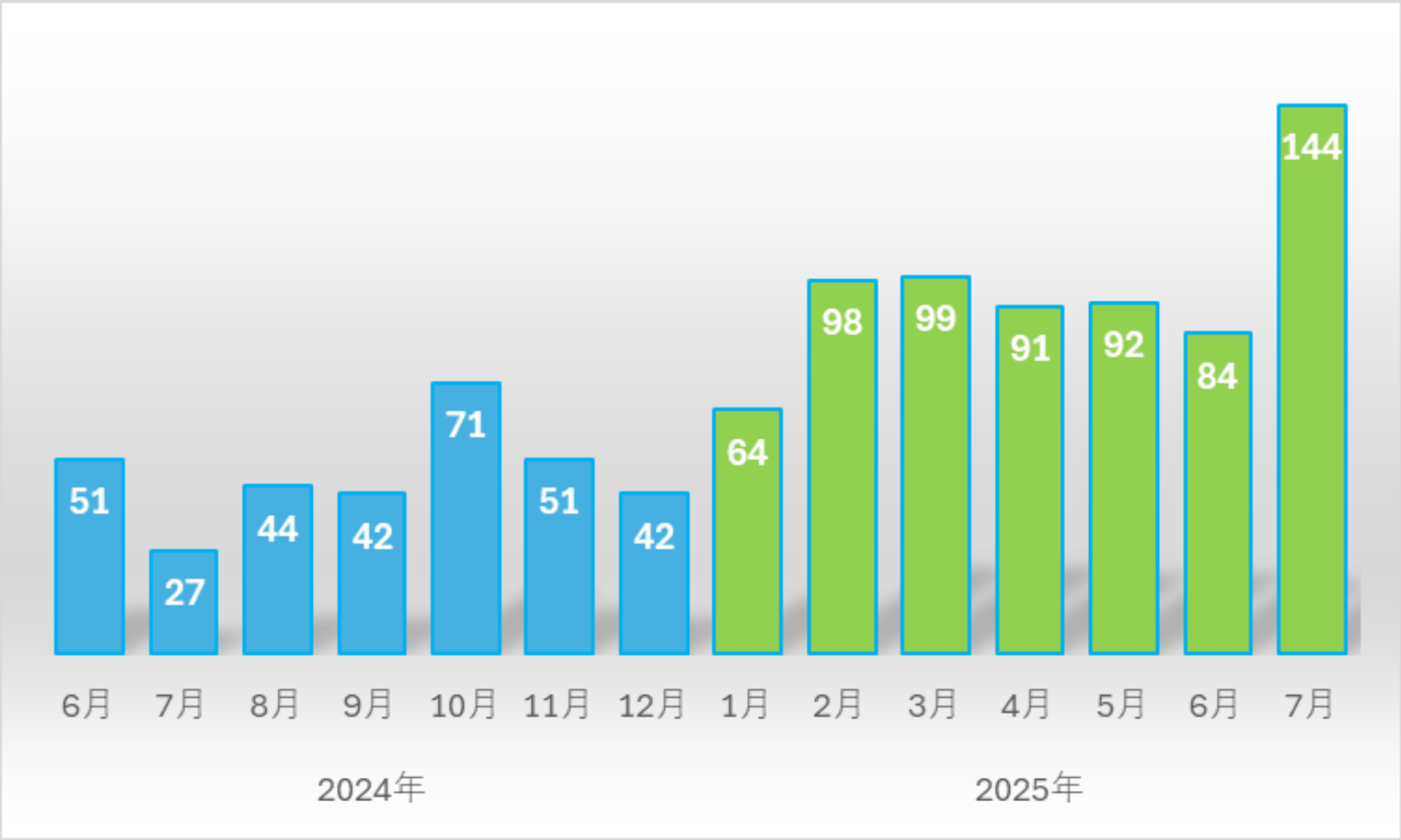
2025年9月5日 14時21分 事件

お笑いタレントやスポーツ選手のインスタグラムのアカウントを乗っ取ったとして32歳の容疑者が不正アクセス禁止法違反の疑いで逮捕されました。警視庁は、乗っ取ったアカウントから女性に性的な画像を要求するメッセージなどを送っていた疑いがあるとみて調べています。

https://www3.nhk.or.jp/news/html/20250905/k10014913731000.html

3.インターネットサービスへの不正ログイン

月別の相談件数



安心相談窓口だより

インターネットサービスへの
不正ログインによる被害が
増加中

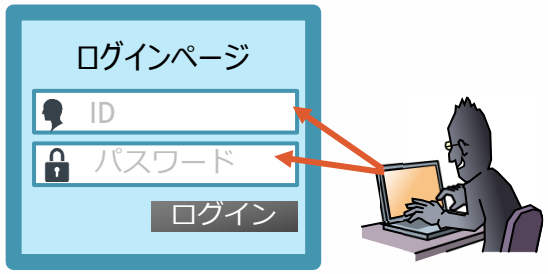
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

3.インターネットサービスへの不正ログイン

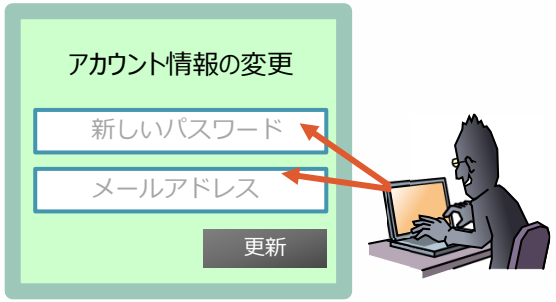
手口

■ InstagramなどのSNSアカウントを乗っ取られたという相談が多数

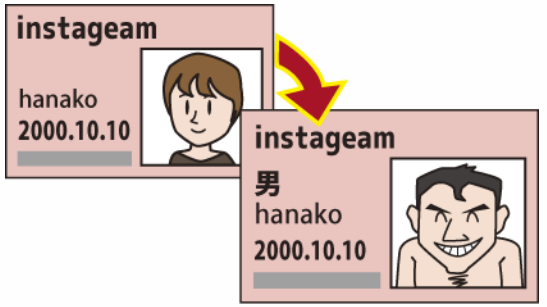
①攻撃者が被害者の
パスワードを破る(特定する)



②被害者のID/PW
を使って**不正ログイン**



③PWとメールアドレスを変更



- プロフィールを変えられた
- アカウントにログインできない!
- PWの再設定メールが来ない!!

アカウントの乗っ取りはパスワードを破られることから始まる

3.インターネットサービスへの不正ログイン

手口

■ パスワードを破る

- パスワードでよく使われる言葉などを集めた専用の辞書を利用する「辞書攻撃」。
- すべての文字列の組み合わせを試す「総当たり攻撃」

「ログインパスワード」に意味のある単語や、
自分に関連の深い語句を使うと、
辞書攻撃などによってパスワードを破られる

■ 国家サイバー統括室（NCO） インターネットの安全・安心ハンドブック
https://security-portal.nisc.go.jp/guidance/handbook.html

3.インターネットサービスへの不正ログイン

手口

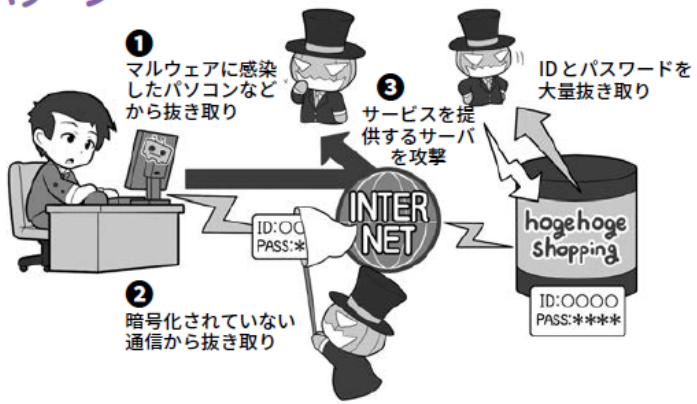
■ 漏えいしたパスワードを悪用する

- 流出した名簿やID・パスワードのリストを入力して試す「リスト型攻撃（アカウントリスト攻撃・パスワードリスト攻撃）」など。

さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

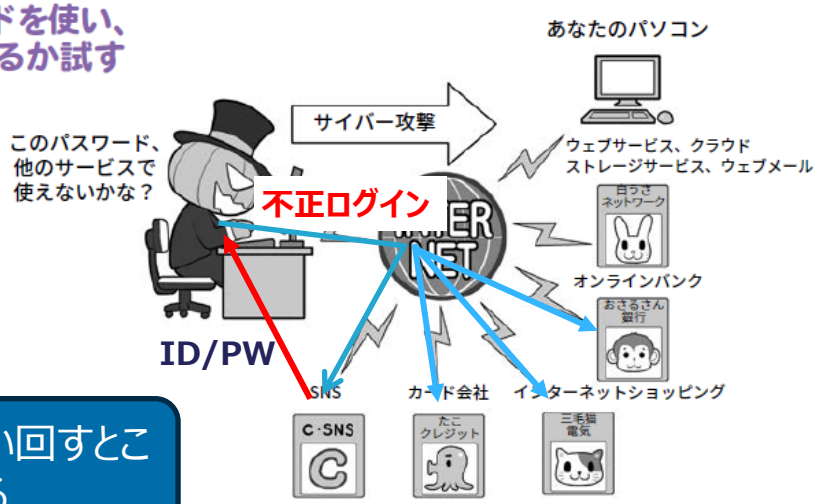
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回し▶用語集 P.201や、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



同じパスワードを複数のサイトで使い回すとこの被害に遭う可能性がある

3.インターネットサービスへの不正ログイン

手口

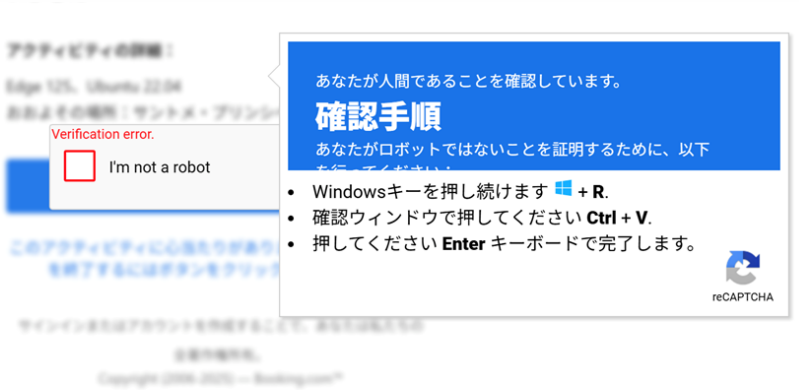
■ 被害者から、他人に教えてはいけない**本人確認情報**を聞き出す

3.マルウェアによる認証情報の窃取（参考）ClickFix

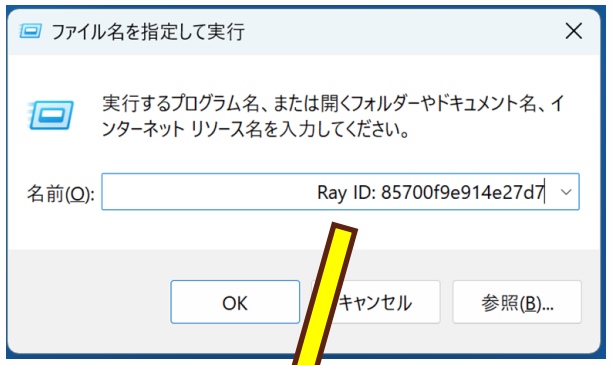
偽サイトでの認証や警告から、解決方法（Fix）が表示され、
手順通り操作すると、ウイルス感染させられるという手口

1.認証画面を操作するが

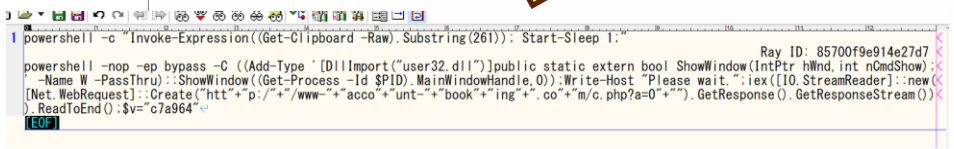
2.エラーになり確認手順が表示



3.手順を操作するとウイルス感染に誘導するコマンドを実行



実行されるコマンド



- 端末内の認証情報を窃取するインフォスティーラーと総称されるウイルスへの感染報告あり
- 窃取した認証情報を使って不正ログインされる可能性がある

3.インターネットサービスへの不正ログイン

対策

- アカウントの適切な作成と管理
  - パスワードは「長く」「複雑で」「使いまわさない」
  - 多要素認証を設定する
- フィッシングサイトにID・パスワードを入力しない
  - パスワード入力は慎重に
- 本人確認情報を他人に教えない
  - 共有しないように注意が書かれている。必ず守る。

3.インターネットサービスへの不正ログイン

対策

- パスワードを「長く」、「複雑」にし、「使い回さない」
- 総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段です。
- **数字＋英大文字・英小文字**を組み合わせて**できるだけ長い文字数**（15桁程度）を推奨します。
- より安全性を高めたい場合は記号を追加してください。
- 桁数や文字種が増えるほど安全性は高まります。

ログイン用パスワードは、長くすることでより安全に

「数字＋英大文字＋英小文字」の８桁だと→約218兆通り
「数字＋英大文字＋英小文字」の12桁だと→約32垓通り

同じ文字種でも、パスワードを長く設定することで推認されにくくなります。

3.インターネットサービスへの不正ログイン

対策

短い日本語のフレーズを決定
テレビが大好き

決めたフレーを ローマ字に変換
terebigadaisuki

変換ルール1を適用（大文字に変換）
terebiGAdaisuki

変換ルール2を適用（末尾に数字を追加）
terebiGAdaisuki06

変換ルール3を適用（末尾に記号を追加）
terebiGAdaisuki06&&

より安全性を高めたい場合

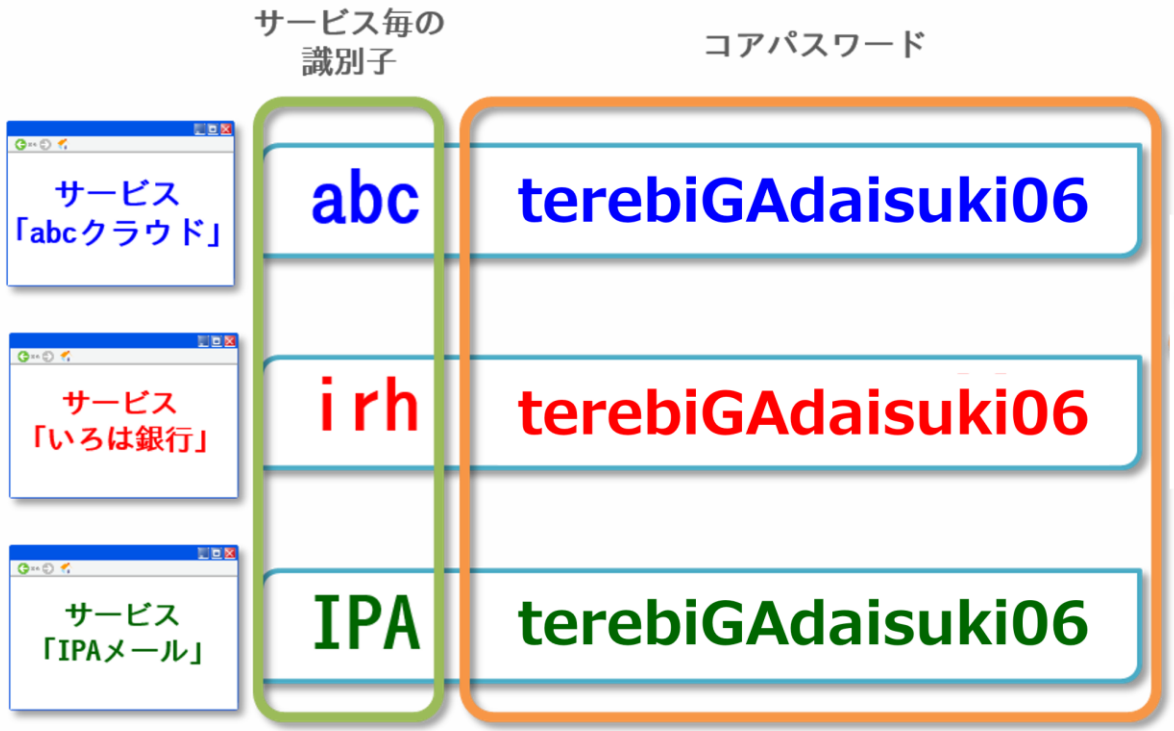
使い回しを回避するパスワードの作成・管理例
～①コアパスワードの作成～

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

3.インターネットサービスへの不正ログイン

対策

使い回しを回避するパスワードの作成・管理例
～②サービス毎に異なるパスワードの作成～



https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

3.インターネットサービスへの不正ログイン

対策

使い回しを回避するパスワードの作成・管理例
③パスワードの管理方法～

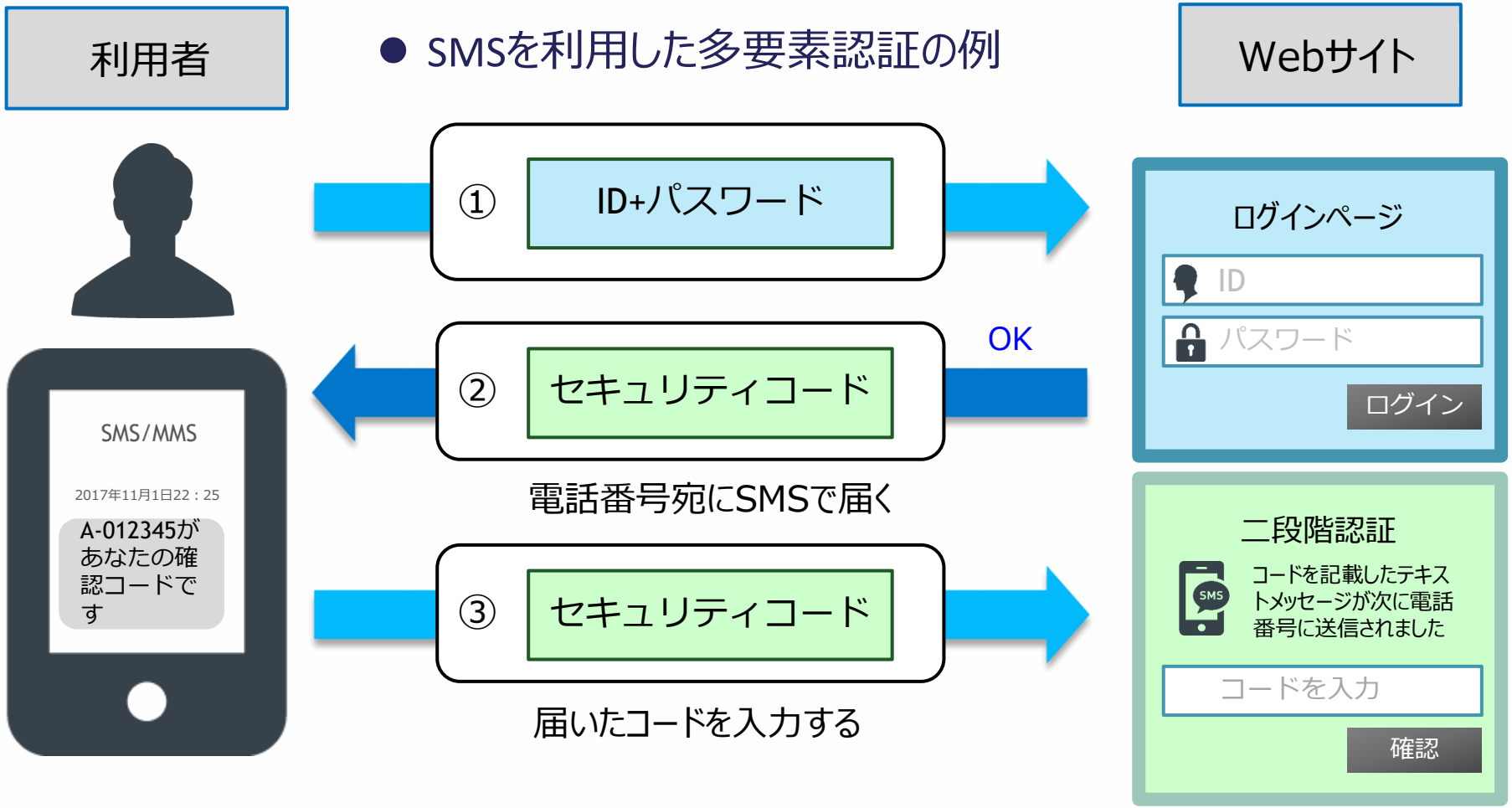
これらの情報を電子ファイルなどで保存

※コアパスワードは、別途、紙などで管理

3.インターネットサービスへの不正ログイン

対策

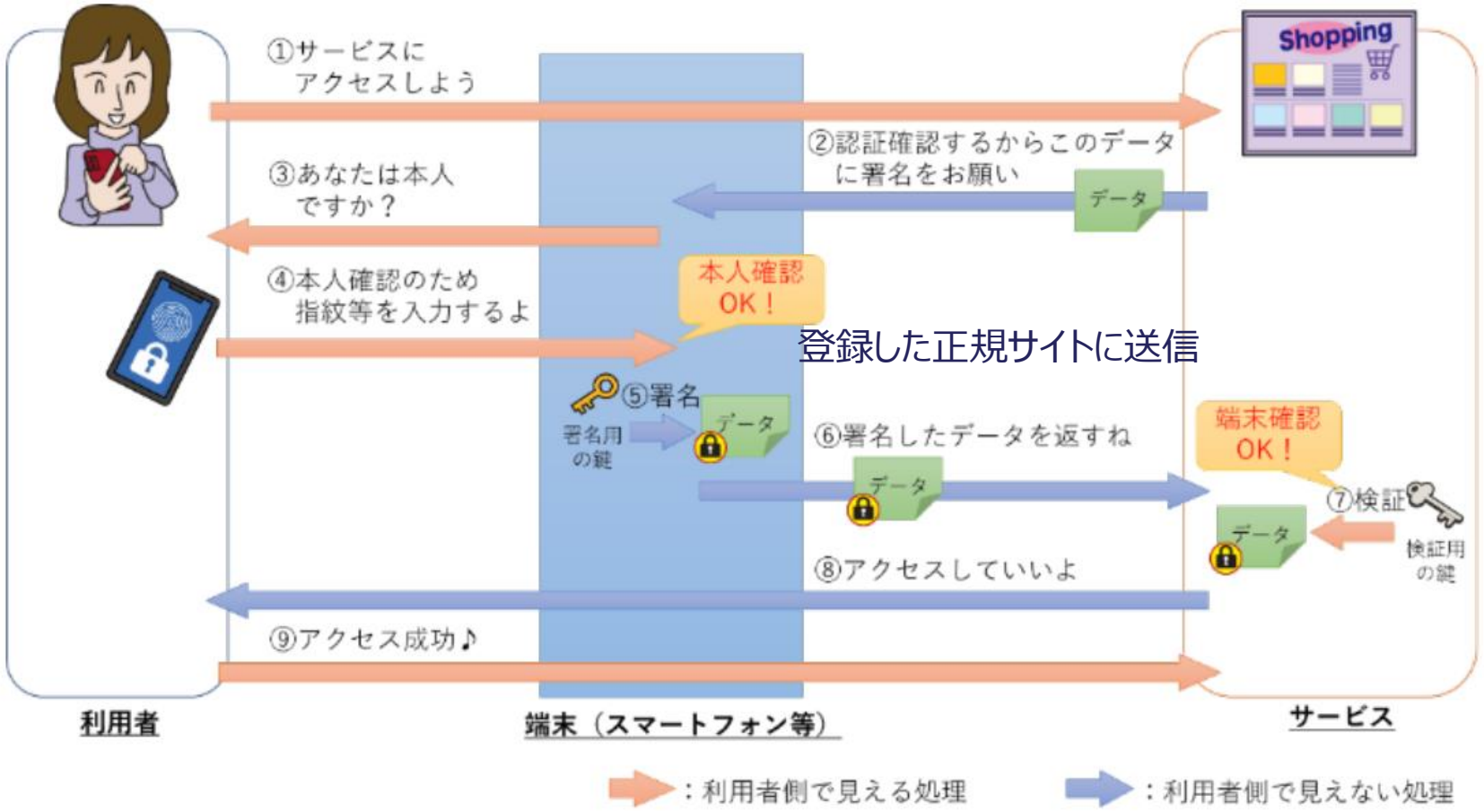
多要素認証を利用



3.インターネットサービスへの不正ログイン

対策

パスキー認証



パスキー認証では

- **パスワードを送信しない**
  → パスワードを盗めない
- **本人を証明する署名データは事前に登録した正規サイトにしか送信しない**
  → リアルタイムフィッシングで盗めない

https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf P34【パスキーとは】

3.インターネットサービスへの不正ログイン

対策

■ ２要素認証、パスキーを採用しているサービス例

- Googleアカウント（２段階認証プロセス、パスキー）
- Apple ID（2ファクタ認証）
- Microsoft アカウント（２段階認証、パスキー）
- Yahoo! JAPAN ID（ワンタイムパスワード、パスキー）
- Amazon（２段階認証、パスキー）
- Facebook （２段階認証、パスキー）
- Instagram（２段階認証）
- X（旧Twitter） （２要素認証、パスキー）
- メルカリ（２段階認証、パスキー）

4.サイバーセキュリティ対策9か条

4.サイバーセキュリティ対策9か条

インターネットの
安全・安心
ハンドブック

https://security-portal.nisc.go.jp/guidance/handbook.html

- 国家サイバー統括室（NCO）
- 協力
  - 警察庁
  - 総務省
  - 経済産業省
  - 情報処理推進機構

サイバーセキュリティ対策9か条

IPA

1 OSやソフトウェアは常に最新の状態にしておこう

最新の攻撃に対抗するため、OSやソフトウェアメーカーが提供している修正用アップデートを常に適用しましょう。

2 パスワードは長く複雑にして、他と使い回さないようにしよう

パスワードは長く複雑にし、機器やサービス間で使い回さないことを徹底して安全性を高めましょう。

3 多要素認証を利用しよう

サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

4 偽メールや偽サイトに騙されないように用心しよう

フィッシング詐欺メールは年々手口が巧妙になっています。心当たりがあるものでもメールやメッセージのURLには安易にアクセスしないようにしましょう。

5 メールの添付ファイルや本文中のリンクに注意しよう

心当たりのない送信元からのメールに添付されているファイルやリンクはもちろん、ファイルやリンクを開かせようとするものには注意しましょう。

6 スマホやPCの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るには、まず待ち受け画面をロックすることが第一です。短時間であっても端末を手元から離す際はロックを忘れないようにしましょう。

7 大切な情報は失う前にバックアップ（複製）しよう

大切な情報を失っても、バックアップから復元することで被害を軽減することができます。普段からバックアップして攻撃や天災に備えましょう。

8 外出先では紛失・盗難・覗き見に注意しよう

外出先でスマホやパソコンを使う時は、背後からの覗き見に注意しましょう。また、紛失・盗難の危険があるので、公共の場でスマホを放置することは絶対にやめましょう。

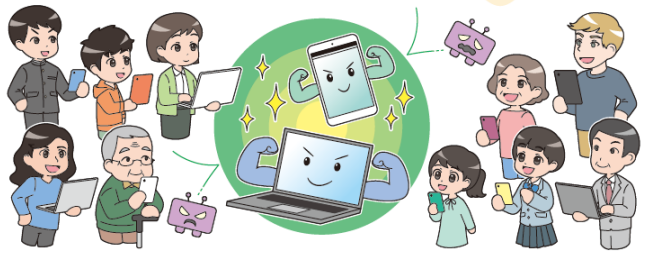
9 困った時はひとりで悩まず、まず相談しよう

インターネットでの被害に遭遇したら、ひとりで悩まず各種相談窓口に相談しましょう。

インターネットを安全・安心に利用するための

NISC IPA

サイバーセキュリティ対策 9 か条



https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

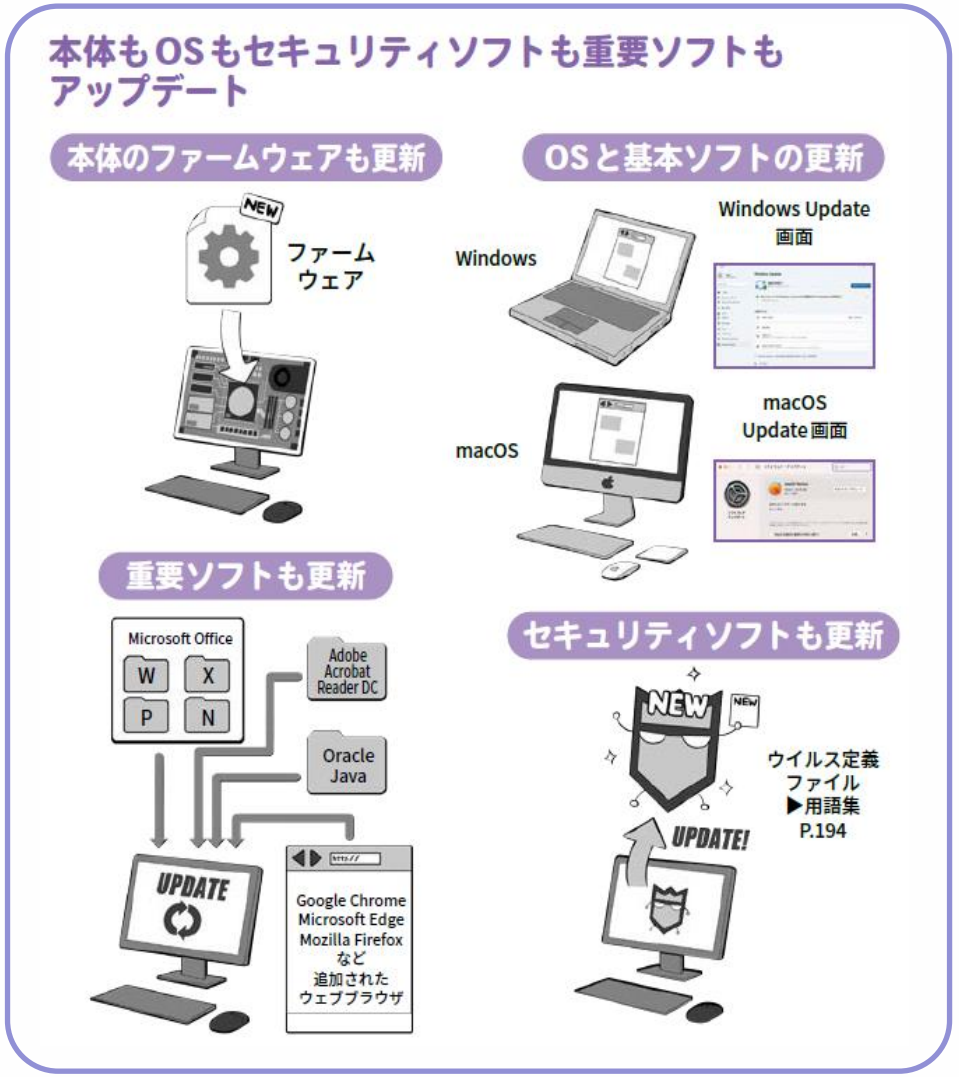
1.OSやソフトウェアは常に最新の状態にしておこう

1 OSやソフトウェアは常に最新の状態にしておこう

最新の攻撃に対抗するため、OSやソフトウェアメーカーが提供している修正用アップデートを常に適用しましょう。

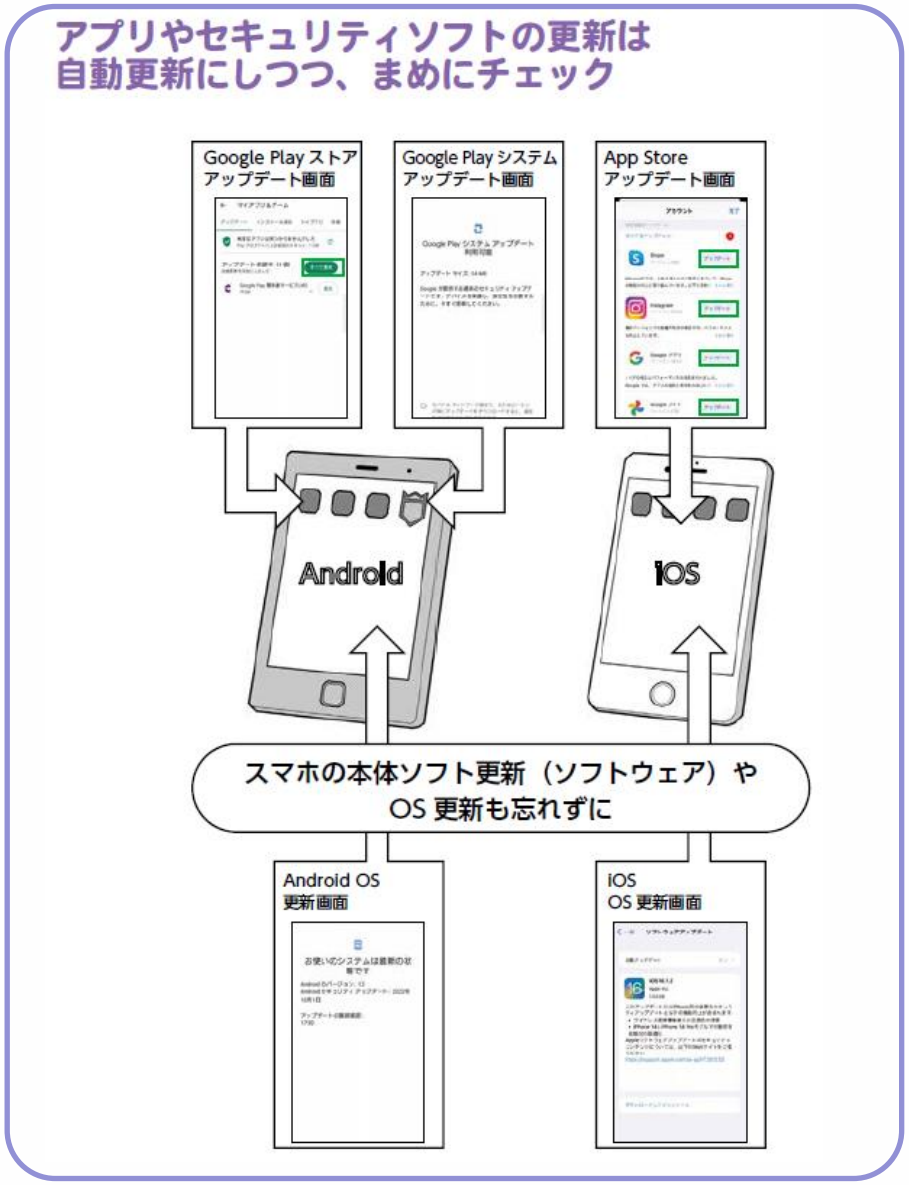
1.OSやソフトウェアは常に最新の状態にしておこう

- 悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデートを行いましょう。
- 最近の機種では、OS 関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出ます。
- セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しましょう。



1.OSやソフトウェアは常に最新の状態にしておこう

- スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。
- 機器本体のファームウェアのアップデートでも、OS のアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。



1.OSやソフトウェアは常に最新の状態にしておこう

- また、ネットワークにつながるルータやIoT機器、スマート家電なども脆弱性を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。

- ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えしましょう。

ネットにつながるIT機器（ルータやIoT機器）もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと

無線LANアクセスルータ

ネットワーク対応プリンタ

ネットワークカメラ

9.困った時はひとりで悩まず、まず相談しよう

9 困った時はひとりで悩まず、まず相談しよう

インターネットでの被害に遭遇したら、ひとりで悩まず各種相談窓口に相談しましょう。

9.困った時はひとりで悩まず、まず相談しよう

- 周りの友達
- 公的機関の相談窓口
- サービス事業者
- インターネット検索

https://www.ipa.go.jp/security/anshin/index.html

https://www.kokusen.go.jp/map/

https://www.npa.go.jp/bureau/cyber/index.html

情報提供

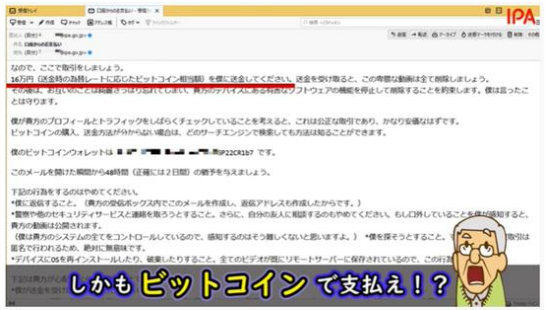
■ 安心相談窓口だより

- 「安心相談窓口だより」では、IPAの情報セキュリティ安心相談窓口に寄せられる相談内容などをもとに、情報セキュリティに関するさまざまテーマをピックアップして紹介していきます。
- 被害防止に向けた自己学習や普及啓発のための資料などとして活用してください。
- 「安心相談窓口だより」は不定期で公開・更新します。

https://www.ipa.go.jp/security/anshin/attention/index.html

情報提供

■ YouTube　手口検証動画シリーズ



- よくある手口に引っかかる様子を動画で分かりやすく説明しています。
- 実存した詐欺サイトにて手口検証したリアリティのある内容です。

https://www.ipa.go.jp/security/anshin/verificationmov.html

情報提供

■ Xアカウント（Twitter）

https://twitter.com/IPA_anshin

■ Facebookアカウント

https://www.facebook.com/ipa.anshin

■ 質疑・応答

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan